1

Le groupe linéaire en dimension finie

[1]Pour ce chapitre $\mathbb{K}$ désigne un corps commutatif et E est un $\mathbb{K}$-espace vectoriel de dimension $n \geq 1$.

$E^* = \mathcal{L}(E, \mathbb{K})$ est l'espace dual de E.

$\mathcal{L}(E)$ est l'algèbre des endomorphismes de E, $GL(E) = (\mathcal{L}(E))^\times$ est le groupe des éléments inversibles de $\mathcal{L}(E)$, soit le groupe des automorphismes de E.

Le transposé (ou adjoint) de $u \in \mathcal{L}(E)$ est l'endomorphisme ${}^t u \in \mathcal{L}(E^*)$ défini par :

$$\forall \varphi \in E^*, \quad {}^t u(\varphi) = \varphi \circ u$$

Pour tout entier $n \geq 1$, $\mathcal{M}_n(\mathbb{K})$ désigne l'algèbre des matrices carrées d'ordre n à coefficients dans $\mathbb{K}$ et $GL_n(\mathbb{K})$ le groupe des éléments inversibles de $\mathcal{M}_n(\mathbb{K})$, soit le groupe des matrices inversibles de $\mathcal{M}_n(\mathbb{K})$.

Pour E de dimension $n \geq 1$, le choix d'une base de E permet de réaliser un isomorphisme d'algèbres de $\mathcal{L}(E)$ sur $\mathcal{M}_n(\mathbb{K})$ et cet isomorphisme induit un isomorphisme de groupes de $GL(E)$ sur $GL_n(\mathbb{K})$.

On note Id [resp. I_n] l'endomorphisme [resp. la matrice] identité.

Une matrice scalaire est une matrice diagonale de la forme λI_n, où $\lambda \in \mathbb{K}$.

Une homothétie est un endomorphisme de E de la forme λId, où $\lambda \in \mathbb{K}$.

Pour tout entier $n \geq 1$, on désigne par $(e_k)_{1 \leq k \leq n}$ la base canonique de $\mathbb{K}^n$ et par $(E_{ij})_{1 \leq i,j \leq n}$ celle de $\mathcal{M}_n(\mathbb{K})$, où les matrices E_{ij} sont définies par :

$$\forall k \in \{1, \cdots, n\}, \ E_{ij} e_k = \begin{cases} 0 \text{ si } k \neq j \\ e_i \text{ si } k = j \end{cases}$$

(la colonne $k \neq j$ de E_{ij} est nulle et la colonne j a tous ses termes nuls sauf celui en ligne i qui vaut 1), ou encore :

$$E_{ij} = (0, \cdots, 0, e_i, 0, \cdots, 0)$$

le vecteur e_i étant placé en colonne j, soit $(E_{ij})_{pq} = \delta_{ip}\delta_{qj}$, où δ_{rs} est le symbole de Kronecker.

On vérifie facilement (exercice **??**) que :

$$\begin{cases} E_{ij} E_{jk} = E_{ik} \\ E_{ij} E_{pk} = 0 \text{ si } j \neq p \end{cases}$$

1. Version du 20/09/2016

1.1 Premières propriétés

Le théorème qui suit nous donne des définitions équivalentes du groupe linéaire $GL(E)$.

Théorème 1.1 *Pour $u \in \mathcal{L}(E)$, les assertions suivantes sont équivalentes :*

1. $u \in GL(E)$;
2. $\ker(u) = \{0\}$ *(ce qui revient à dire que u est injectif)* ;
3. $\mathrm{Im}(u) = E$ *(ce qui revient à dire que u est surjectif)* ;
4. $\mathrm{rg}(u) = n$;
5. $\det(u) \neq 0$;
6. *u transforme toute base de E en une base de E* ;
7. *il existe $v \in \mathcal{L}(E)$ tel que $u \circ v = Id$ (u admet un inverse à droite)* ;
8. *il existe $w \in \mathcal{L}(E)$ tel que $w \circ u = Id$ (u admet un inverse à gauche).*

Démonstration. Cela se déduit facilement des définitions et du théorème du rang. ∎

Pour E de dimension infinie, certaines de ces équivalences ne sont plus vraies.

La condition $v \circ u = Id$ nous dit seulement que u est injectif ($\ker(u) = \{0\}$) et que v est surjectif (pour tout $y \in E$, on a $y = v(u(y))$).

Dans le cas où E est de dimension infinie dénombrable (par exemple $E = \mathbb{K}[X]$), en désignant par $(e_n)_{n\in\mathbb{N}}$ une base de E, l'application linéaire u [resp. v] définie par $u(e_n) = e_{n+1}$ pour tout $n \in \mathbb{N}$ [resp. $v(e_0) = 0$ et $v(e_n) = e_{n-1}$ pour tout $n \in \mathbb{N}^*$) est injective (elle transforme une base en système libre) et non surjective (e_0 n'a pas d'antécédent) [resp. surjective (elle transforme une base en un système générateur) et non injective ($e_0 \in \ker(v)$)] et on a $v \circ u = Id$.

Mais, on a quand même le résultat suivant, valable en toute dimension.

Théorème 1.2 *Si $u \in \mathcal{L}(E)$ admet un unique inverse à gauche [resp. à droite], il est alors inversible.*

Démonstration. Supposons qu'il existe un unique $v \in \mathcal{L}(E)$ tel que $v \circ u = Id$ [resp. $u \circ v = Id$].

Dans ce cas, on a $u \circ v \circ u = u$, soit $(u \circ v - Id) \circ u = 0$ [resp. $u \circ (v \circ u - Id) = 0$].

En posant $w = u \circ v - Id$ [resp. $w = v \circ u - Id$], on a $w \circ u = 0$ et $v \circ u = Id$ [resp. $u \circ w = 0$ et $u \circ v = Id$], ce qui donne par addition, $(v + w) \circ u = Id$ [resp. $u \circ (v + w) = Id$], c'est-à-dire que $v + w$ est un inverse à gauche [resp. à droite] de u, donc $v + w = v$ (unicité d'un tel inverse) et $w = 0$, soit $u \circ v = Id$ [resp. $v \circ u = Id$], ce qui signifie que $u \in GL(E)$ avec $u^{-1} = v$. ∎

L'équivalence entre u transforme toute base de E en une base de E et $u \in GL(E)$ est encore vraie en dimension infinie.

Si $u \in GL(E)$ et $\mathcal{B} = (e_i)_{i\in I}$ est une base de E, tout $y \in E$ s'écrit :

$$y = u(x) = u\left(\sum_{\text{finie}} x_j e_j\right) = \sum_{\text{finie}} x_j u(e_j)$$

donc $u(\mathcal{B})$ est génératrice.

Si $\sum_{\text{finie}} x_j u(e_j) = 0$, on a alors $\sum_{\text{finie}} x_j e_j = 0$ et tous les x_j sont nuls, donc $u(\mathcal{B})$ est libre.

Réciproquement soit $\in \mathcal{L}(E)$ qui transforme toute base de E en une base de E.

S'il existe $x \neq 0$ tel que $u(x) = 0$, on complète $\{x\}$ en une base $\mathcal{B} = \{x\} \cup \mathcal{B}'$ de E telle que $u(\mathcal{B}) = \{0\} \cup u(\mathcal{B}')$ n'est pas une base de E, ce qui contredit l'hypothèse de départ.

Donc u est injectif.
Si $\mathcal{B}$ est une base de E, comme $u(\mathcal{B})$ en est aussi une tout $y \in E$ s'écrit $y = \sum_{\text{finie}} x_j u(e_j) = u\left(\sum_{\text{finie}} x_j e_j\right)$, ce qui signifie que u est surjective.

Exercice 1.1

1. *Montrer que si $u \in GL(E)$, on a alors $u^{-1} \in \mathbb{K}[u]$.*
2. *Le résultat précédent est-il valable en dimension infinie ?*
3. *Montrer que si F est un sous-espace vectoriel de $\mathcal{L}(E)$ contenant Id et stable par la composition des endomorphismes, l'ensemble $G = F \cap GL(E)$ est alors un sous-groupe de $GL(E)$.*

Solution 1.1 *Voir l'exercice* **??**.

Exercice 1.2 *On suppose que $n \geq 2$.*

1. *Montrer que pour toute forme linéaire ℓ sur $\mathcal{M}_n(\mathbb{K})$, il existe une unique matrice $B \in \mathcal{M}_n(\mathbb{K})$ telle que :*
$$\forall A \in \mathcal{M}_n(\mathbb{K}),\ \ell(A) = \operatorname{Tr}(AB)$$
ce qui signifie que l'application linéaire :
$$\begin{array}{rccc} \varphi : & \mathcal{M}_n(\mathbb{K}) & \to & (\mathcal{M}_n(\mathbb{K}))^* \\ & B & \mapsto & \varphi(B) : A \mapsto \operatorname{Tr}(AB) \end{array}$$
est un isomorphisme.
2. *En déduire que pour tout hyperplan H de $\mathcal{M}_n(\mathbb{K})$, on a $H \cap GL_n(\mathbb{K}) \neq \emptyset$ ($GL_n(\mathbb{K})$ coupe tout hyperplan de $\mathcal{M}_n(\mathbb{K})$).*

Solution 1.2 *Pour $n = 1$, on a $\mathcal{M}_n(\mathbb{K}) = \mathbb{K}$, $GL_n(\mathbb{K}) = \mathbb{K}^*$ et $H = \{0\}$, donc $H \cap GL_n(\mathbb{K}) = \emptyset$.*

1. *Pour toute forme linéaire ℓ sur $\mathcal{M}_n(\mathbb{K})$, il existe des scalaires $c_{ij} \in \mathbb{K}$ tels que :*
$$\forall A = ((a_{ij}))_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{K}),\ \ell(A) = \sum_{1 \leq i,j \leq n} c_{ij} a_{ij}$$
En désignant par B la matrice $B = {}^t((c_{ij}))_{1 \leq i,j \leq n}$, on a :
$$(AB)_{ii} = \sum_{j=1}^{n} a_{ij} b_{ji} = \sum_{j=1}^{n} a_{ij} c_{ij}\ \ (1 \leq i \leq n)$$
donc :
$$\ell(A) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} c_{ij} = \sum_{i=1}^{n} (AB)_{ii} = \operatorname{Tr}(AB)$$
et $\ell = \varphi(B)$.
L'application linéaire φ est donc surjective et comme les espaces $\mathcal{M}_n(\mathbb{K})$ et $(\mathcal{M}_n(\mathbb{K}))^*$ sont de même dimension, c'est un isomorphisme.
On peut aussi vérifier que φ est injective en utilisant la base canonique $(E_{ij})_{1 \leq i;j \leq n}$ de

$\mathcal{M}_n(\mathbb{K})$.
Si $B \in \mathcal{M}_n(\mathbb{K})$ *est telle que* $\varphi(B) = 0$, *on a alors* $\mathrm{Tr}(E_{ij}B) = 0$ *pour tous* i, j *compris entre* 1 *et* n *avec :*

$$E_{ij}B = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ b_{j1} & \cdots & \cdots & b_{jn} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix} \longleftarrow \textit{ligne } i$$

ce qui nous donne $b_{ji} = \mathrm{Tr}(E_{ij}B) = 0$.

2. *Si* H *est un hyperplan de* $\mathcal{M}_n(\mathbb{K})$, *il existe alors une forme linéaire non nulle* ℓ *sur* $\mathcal{M}_n(\mathbb{K})$ *telle que* $H = \ker(\ell)$.
Une telle forme est définie par :

$$\forall A = ((a_{ij}))_{1\leq i,j\leq n} \in \mathcal{M}_n(\mathbb{K}),\ \ell(A) = \mathrm{Tr}(AB)$$

avec $B = ((b_{ij}))_{1\leq i,j\leq n} \neq 0$ *dans* $\mathcal{M}_n(\mathbb{K})$.
Il s'agit alors de justifier l'existence de $A \in GL_n(\mathbb{K})$ *telle que* $\mathrm{Tr}(AB) = 0$.
Pour tous i, j *compris entre* 1 *et* n, *on a alors*

$$\ell(E_{ij}) = \mathrm{Tr}(E_{ij}B) = \mathrm{Tr}\begin{pmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ b_{j1} & \cdots & \cdots & b_{jn} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix} = b_{ji}$$

et pour tout scalaire λ *:*

$$\ell(I_n + \lambda E_{ij}) = \mathrm{Tr}(B + \lambda E_{ij}B) = \mathrm{Tr}(B) + \lambda b_{ji}$$

Si la matrice B *n'est pas diagonale, il existe alors* $i \neq j$ *tels que* $b_{ji} \neq 0$, *de sorte que* $I_n + \lambda E_{ij} \in GL_n(\mathbb{K})$ *(son déterminant vaut* 1*) et on aura :*

$$\ell(I_n + \lambda E_{ij}) = \mathrm{Tr}(B) + \lambda b_{ji} = 0$$

pour $\lambda = -\dfrac{\mathrm{Tr}(B)}{b_{ji}}$.
Pour $B = \mathrm{diag}(\lambda_1, \cdots, \lambda_n)$ *diagonale non nulle, on a :*

$$\forall A \in \mathcal{M}_n(\mathbb{K}),\ AB = \begin{pmatrix} \lambda_1 a_{1,1} & \lambda_2 a_{1,2} & \cdots & \lambda_n a_{1,n} \\ \lambda_1 a_{2,1} & \lambda_2 a_{2,2} & \cdots & \lambda_n a_{2,n} \\ \vdots & \ddots & \ddots & \vdots \\ \lambda_1 a_{n,1} & \lambda_2 a_{n,2} & \cdots & \lambda_n a_{n,n} \end{pmatrix}$$

et toute matrice $A \in GL_n(\mathbb{K})$ *telle que* $a_{ii} = 0$ *pour tout* i *compris entre* 1 *et* n *est dans* H. *Par exemple la matrice de permutation :*

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

convient.
On peut aussi raisonner en utilisant le rang de B.
Comme B est non nulle son rang r est non nul et elle est équivalente à la matrice $B_r = \begin{pmatrix} I_r & 0_{r,n-r} \\ 0_{n-r,r} & 0_{n-r,n-r} \end{pmatrix}$, ce qui signifie qu'il existe P, Q dans $GL_n(\mathbb{K})$ telles que $B = PB_rQ$,
ce qui nous donne pour toute matrice $A \in \mathcal{M}_n(\mathbb{K})$:

$$\ell(A) = \mathrm{Tr}(APB_rQ) = \mathrm{Tr}(QAPB_r)$$

et il s'agit de trouver $A' \in GL_n(\mathbb{K})$ (donc $A = Q^{-1}A'P^{-1} \in GL_n(\mathbb{K})$) telle que $\mathrm{Tr}(A'B_r) = 0$.
La matrice de permutation :

$$A' = \begin{pmatrix} 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

convient.

Exercice 1.3 *On suppose pour cet exercice que le corps $\mathbb{K}$ est de caractéristique différente de 2.*

1. *Montrer qu'il existe une base de $\mathcal{L}(E)$ formée d'automorphismes.*
2. *Pour $\mathbb{K} = \mathbb{C}$, déduire le résultat précédent de la densité de $GL(E)$ dans $\mathcal{L}(E)$.*
3. *Pour $\mathbb{K} = \mathbb{C}$, montrer la densité de $GL(E)$ dans $\mathcal{L}(E)$ en utilisant le résultat de la première question.*

Solution 1.3

1. *Pour $n = 1$, c'est clair (tout élément de $GL(E) \backsimeq \mathbb{K}^*$ est base de $\mathcal{L}(E) \backsimeq \mathbb{K}$).*
Pour $n \geq 2$, à toute base $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ de E, on associe la base $(u_{ij})_{1 \leq i,j \leq n}$ de $\mathcal{L}(E)$ définie par :

$$u_{ij}(e_k) = \delta_{j,k}e_i = \begin{cases} 0 \text{ si } k \neq j \\ e_i \text{ si } k = j \end{cases} \quad (1 \leq i, j, k \leq n)$$

(la matrice E_{ij} dans la base $\mathcal{B}$ de u_{ij} a tous les termes nuls sauf celui en ligne i et colonne j qui vaut 1 et $(E_{ij})_{1 \leq i,j \leq n}$ est la base canonique de $\mathcal{M}_n(\mathbb{K})$).
On vérifie alors que la famille d'automorphismes :

$$\mathcal{B} = \{Id\} \cup \{Id + u_{ii},\ 2 \leq i \leq n\} \cup \{Id + u_{ij},\ 1 \leq i \neq j \leq n\}$$

est une base de $\mathcal{L}(E)$ (comme $\mathbb{K}$ est de caractéristique différente de 2, on a bien $\mathcal{B} \subset GL(E)$).
L'égalité :

$$a_{11}Id + \sum_{i=2}^{n} a_{ii}(Id + u_{ii}) + \sum_{1 \leq i \neq j \leq n} a_{ij}(Id + u_{ij}) = 0$$

s'écrit :

$$\left(\sum_{i=1}^{n} a_{ii}\right) Id + \sum_{i=2}^{n} a_{ii}u_{ii} + \left(\sum_{1 \leq i \neq j \leq n} a_{ij}\right) Id + \sum_{1 \leq i \neq j \leq n} a_{ij}u_{ij} = 0$$

soit en notant $\alpha = \sum_{i=1}^{n} a_{ii}$, $\beta = \sum_{1 \leq i \neq j \leq n} a_{ij}$ *et tenant compte de* $Id = \sum_{i=1}^{n} u_{ii}$ *:*

$$(\alpha + \beta)\, u_{11} + \sum_{i=2}^{n} (\alpha + \beta + a_{ii})\, u_{ii} + \sum_{1 \leq i \neq j \leq n} a_{ij} u_{ij} = 0$$

ce qui donne $a_{ij} = 0$ *pour* $1 \leq i \neq j \leq n$, $\beta = 0$, $\alpha = 0$, $a_{ii} = 0$ *pour* $2 \leq i \leq n$ *et* $a_{11} = 0$.

2. *Pour* $\mathbb{K} = \mathbb{C}$, $V = \mathrm{Vect}\,(GL\,(E))$ *est un sous espace vectoriel fermé de* $\mathcal{L}\,(E)$ *(on est en dimension finie) qui contient* $GL\,(E)$, *il contient donc son adhérence c'est-à-dire* $\mathcal{L}\,(E)$. *Donc* $V = \mathcal{L}\,(E)$ *et du système générateur* $GL\,(E)$ *on peut extraire une base.*
3. *En désignant par* $(v_{ij})_{1 \leq i,j \leq n}$ *une base de* $\mathcal{L}\,(E)$ *formée d'automorphismes, tout endomorphisme* $u \in \mathcal{L}\,(E)$ *s'écrit* $u = \sum_{1 \leq i,j \leq n} a_{ij} v_{ij}$ *et il n'existe qu'un nombre fini d'entiers* $k \geq 1$ *tels que* $\det\left(\sum_{1 \leq i,j \leq n} \left(a_{ij} + \frac{1}{k}\right) v_{ij}\right) = 0$ *(la fonction polynomiale* $\lambda \mapsto \det\left(\sum_{1 \leq i,j \leq n} (a_{ij} + \lambda)\, v_{ij}\right)$ *n'a qu'un nombre fini de racines complexes), il existe donc un entier* $k_0 \geq 1$ *tel que* $u_k = \sum_{1 \leq i,j \leq n} \left(a_{ij} + \frac{1}{k}\right) v_{ij} \in GL\,(E)$ *pour tout* $k \geq k_0$ *et on a* $u = \lim_{k \to +\infty} u_k$.

1.2 Sous-groupes de $GL\,(E)$

$SL\,(E)$ [resp. $SL_n\,(\mathbb{K})$] est le sous-ensemble de $\mathcal{L}\,(E)$ [resp. de $\mathcal{M}_n\,(\mathbb{K})$] défini par :

$$SL\,(E) = \{u \in \mathcal{L}\,(E) \mid \det(u) = 1\}$$

$$SL_n\,(\mathbb{K}) = \{A \in \mathcal{M}_n\,(\mathbb{K}) \mid \det(A) = 1\}$$

On rappelle qu'une suite exacte est la donnée de trois groupes N, G, H et de deux morphismes de groupes :

$$\{1\} \to N \xrightarrow{i} G \xrightarrow{p} H \to \{1\}$$

tels que i est injectif, p est surjectif et $\mathrm{Im}\,(i) = \ker(p)$.

Théorème 1.3 *$SL\,(E)$ est un sous-groupe distingué de $GL\,(E)$ isomorphe à $SL_n\,(\mathbb{K})$ (qui est aussi distingué dans $GL_n\,(\mathbb{K})$), le groupe quotient $\frac{GL\,(E)}{SL\,(E)}$ est isomorphe à $\mathbb{K}^*$ et on a la suite exacte :*

$$\{Id\} \to SL\,(E) \xrightarrow{i} GL\,(E) \xrightarrow{\det} \mathbb{K}^* \to \{Id\}$$

où i est l'injection canonique de $SL\,(E)$ dans $GL\,(E)$.

Démonstration. L'application det étant un morphisme de groupes surjectif de $GL\,(E)$ sur $\mathbb{K}^*$, son noyau $SL\,(E)$ est un sous-groupe distingué de $GL\,(E)$.

Ce morphisme det induit donc un isomorphisme du groupe quotient $\frac{GL\,(E)}{SL\,(E)}$ sur le groupe multiplicatif $\mathbb{K}^*$.

Le choix d'une base de E réalise un isomorphisme de groupes de $SL(E)$ sur $SL_n(\mathbb{K})$.
Il est clair que la suite indiquée est exacte. ■

On rappelle que le centre $Z(G)$ d'un groupe $(G,\cdot)$ [resp. d'un anneau] est :

$$\begin{aligned} Z(G) &= \{g \in G \mid \forall h \in G,\ gh = hg\} \\ &= \left\{g \in G \mid \forall h \in G,\ ghg^{-1} = h\right\} \end{aligned}$$

C'est donc l'ensemble des éléments de G qui commutent à tous les autres.
Ce centre étant le noyau du morphisme de groupes :

$$\begin{array}{cccc} \Phi & G & \to & \mathrm{Aut}(G) \\ & g & \mapsto & \Phi_g : h \mapsto ghg^{-1} \end{array}$$

(les Φ_g sont les automorphismes intérieurs), c'est un sous-groupe distingué de G. Ce sous-groupe est commutatif.

Il est facile de vérifier que si deux groupes sont isomorphes, il en est alors de même de leurs centres.

En effet, si G, G' sont deux groupes et $\varphi : G \to G'$ un isomorphisme de groupes, on a alors :

$$\begin{aligned} (g \in Z(G)) &\Leftrightarrow (\forall h \in G,\ gh = hg) \Leftrightarrow (\forall h \in G,\ \varphi(g)\varphi(h) = \varphi(h)\varphi(g)) \\ &\Leftrightarrow (\forall h' \in G',\ \varphi(g)h' = h'\varphi(g)) \Leftrightarrow (\varphi(g) \in Z(G')) \end{aligned}$$

Il en résulte que φ induit un isomorphisme de groupes de $Z(G)$ sur $Z(G')$.
On note :

$$\mu_n(\mathbb{K}) = \{\lambda \in \mathbb{K} \mid \lambda^n = 1\}$$

l'ensemble des racines n-èmes de l'unité dans $\mathbb{K}^*$.

Lemme 1.1 *$\mu_n(\mathbb{K})$ est un sous-groupe cyclique du groupe multiplicatif $\mathbb{K}^*$.*

Démonstration. $\mu_n(\mathbb{K})$ est le noyau du morphisme de groupes $\varphi_n \in \lambda \in \mathbb{K}^* \mapsto \lambda^n$, c'est donc un sous-groupe fini du groupe multiplicatif $\mathbb{K}^*$ de cardinal au plus égal à n (racines dans $\mathbb{K}$ du polynôme de degré n, $X^n - 1$) et en conséquence il est cyclique. ■

Théorème 1.4 *On a :*

$$Z(GL(E)) = \mathbb{K}^* \cdot Id \text{ et } Z(SL(E)) = \mu_n(\mathbb{K}) \cdot Id$$

Démonstration. Comme $GL(E)$ [resp. $SL(E)$] est isomorphe à $GL_n(\mathbb{K})$ [resp. à $SL_n(\mathbb{K})$], il nous suffit de déterminer les centres de $GL_n(\mathbb{K})$ et $SL_n(\mathbb{K})$.

Une matrice $A = ((a_{ij}))_{1 \le i,j \le n} \in Z(GL_n(\mathbb{K}))$ [resp. $A \in Z(SL_n(\mathbb{K}))$] commute en particulier à toutes les matrices (de transvection) $I_n + E_{ij} \in SL_n(\mathbb{K}) \subset GL_n(\mathbb{K})$ où $1 \le i \ne j \le n$, donc elle commute à toutes les matrices E_{ij} pour $1 \le i \ne j \le n$.

Avec :

$$AE_{ij}e_j = Ae_i = \sum_{k=1}^{n} a_{ki}e_k = E_{ij}Ae_j = E_{ij}\left(\sum_{k=1}^{n} a_{kj}e_k\right) = a_{jj}e_i$$

on déduit que $a_{ki} = 0$ pour $k \ne i$ et $a_{ii} = a_{jj}$, c'est-à-dire que $A = \lambda I_n$ avec $\lambda \in \mathbb{K}^*$ [resp. $\lambda \in \mu_n(\mathbb{K})$] (puisque $\det(A) = \lambda^n \ne 0$ [resp. $\det(A) = \lambda^n = 1$]).

Réciproquement, une telle matrice scalaire est dans $Z(GL_n(\mathbb{K}))$ [resp. dans $Z(SL_n(\mathbb{K}))$].
On a donc $Z(GL_n(\mathbb{K})) = \mathbb{K}^* \cdot I_n$ et $Z(SL(E)) = \mu_n(\mathbb{K}) \cdot Id$. ■

Le groupe $\mu_n(\mathbb{K})$ étant cyclique d'ordre divisant n, il en est de même du centre $Z(SL_n(\mathbb{K}))$.

Pour $\mathbb{K}=\mathbb{C}$:

$$Z\left(SL_n\left(\mathbb{C}\right)\right)=\left\{e^{\frac{2ik\pi}{n}}I_n,\ 0\leq k\leq n-1\right\}$$

est cyclique d'ordre n.

Pour $\mathbb{K}=\mathbb{R}$:

$$Z\left(SL_n\left(\mathbb{R}\right)\right)=\begin{cases}\{I_n\} \text{ si } n \text{ est impair}\\ \{-I_n,I_n\} \text{ si } n \text{ est pair}\end{cases}$$

est cyclique d'ordre 1 ou 2.

On peut vérifier que le centre de $\mathcal{L}\left(E\right)$ est formé des endomorphismes qui laissent stables tous les sous espaces vectoriels de dimension r de E, l'entier r compris entre 1 et $n-1$ étant donné (exercice **??**).

De manière plus générale, on a les résultats suivants pour E de dimension finie ou infinie.

Exercice 1.4 *Pour cet exercice, l'espace vectoriel E est de dimension finie ou infinie et $u\in\mathcal{L}\left(E\right)$.*

1. *Montrer que les assertions suivantes sont équivalentes :*
   - *(a) u est une homothétie ;*
   - *(b) u laisse stable toute droite de E ;*
   - *(c) u laisse stable tout hyperplan de E ;*
   - *(d) ${}^tu$ laisse stable toute droite de E^* ;*
   - *(e) ${}^tu$ est une homothétie.*
2. *Déduire de la question précédente que le centre de l'anneau $\mathcal{L}\left(E\right)$ est $\mathbb{K}\cdot Id$, puis que le centre du groupe multiplicatif $GL\left(E\right)$ est $\mathbb{K}^*\cdot Id$.*

Solution 1.4

1. *$(a)\Rightarrow(b)$ Si u est une homothétie, il laisse alors stable tout sous-espace vectoriel de E, donc toute droite.*
   $(b)\Rightarrow(a)$ Soit $u\in\mathcal{L}\left(E\right)$ qui laisse stable toute droite de E.
   Cela signifie que, pour tout $x\in E\setminus\{0\}$, il existe $\lambda_x\in\mathbb{K}$ tel que $u\left(x\right)=\lambda_x x$.
   En désignant par $(e_i)_{i\in I}$ une base de E, il existe une famille de scalaires $(\lambda_i)_{i\in I}$ telle que :

$$\forall i\in I,\ u\left(e_i\right)=\lambda_i e_i$$

   Pour $i\neq j$ dans I, on a alors :

$$\lambda_{i,j}\left(e_i-e_j\right)=u\left(e_i-e_j\right)=\lambda_i e_i-\lambda_j e_j$$

   où $\lambda_{i,j}\in\mathbb{K}$ et $\lambda_i=\lambda_{i,j}=\lambda_j$ puisque la famille (e_i,e_j) est libre. En notant λ la valeur commune des λ_i, on a $u\left(e_i\right)=\lambda e_i$ pour tout $i\in I$, ce qui revient à dire que $u=\lambda Id_E$.
   $(a)\Rightarrow(c)$ Si u est une homothétie, il laisse alors stable tout sous-espace vectoriel de E, donc tout hyperplan.
   $(c)\Rightarrow(d)$ Soit $u\in\mathcal{L}\left(E\right)$ qui laisse stable tout hyperplan H de E (i. e. pour tout $x\in H$, $u\left(x\right)\in H$).
   Pour toute forme linéaire $\varphi\in E^*\setminus\{0\}$, $H=\ker\left(\varphi\right)$ est un hyperplan de E et pour $a\in E$ tel que $\varphi\left(a\right)\neq 0$, on a $E=\mathbb{K}a\oplus H$, chaque vecteur $x\in E$ s'écrivant $x=\lambda a+h$ avec

$\lambda = \dfrac{\varphi(x)}{\varphi(a)}$ *et* $h = x - \lambda a \in H$.
On a alors, en tenant compte du fait que $u(h) \in H$ *:*

$$ {}^t u(\varphi)(x) = \varphi(u(x)) = \varphi(\lambda u(a) + u(h)) = \lambda\varphi(u(a)) = \frac{\varphi(x)}{\varphi(a)}\varphi(u(a)) = \mu_\varphi\varphi(x) $$

avec $\mu_\varphi = \dfrac{\varphi(u(a))}{\varphi(a)} \in \mathbb{K}$. *On a donc* ${}^t u(\varphi) = \mu_\varphi\varphi$ *et* ${}^t u$ *laisse stable toute droite de* E^*.
$(d) \Rightarrow (e)$ *C'est déjà vu en remplaçant* E *par* E^*.
$(e) \Rightarrow (a)$ *Montrons que si* ${}^t u = \lambda Id_{E^*}$, *on a alors* $u = \lambda Id_E$.
Si $u \neq \lambda Id_E$, *il existe alors un vecteur* $x \in E \setminus \{0\}$ *tel que* $y = u(x) - \lambda x \neq 0$ *et en complétant* y *en une base* $\mathcal{B}$ *de* E, *la forme linéaire* φ *définie par* $\varphi(y) = 1$ *et* $\varphi(e) = 0$ *pour* $e \in \mathcal{B} \setminus \{y\}$ *est telle que* $({}^t u(\varphi) - \lambda\varphi)(x) = \varphi(u(x)) - \lambda\varphi(x) = \varphi(y) = 1$, *ce qui contredit l'égalité* ${}^t u(\varphi) = \lambda\varphi$.

2.

(a) Si u *est dans le centre de* $\mathcal{L}(E)$, *pour tout* $x \in E \setminus \{0\}$ *il commute à un projecteur* p_x *sur la droite* $\mathbb{K}x$ *(parallèlement à un hyperplan* H_x *supplémentaire de* $\mathbb{K}x$*), donc* $p_x(u(x)) = u(p_x(x)) = u(x)$ *et* $u(x) \in \mathbb{K}x$, *ce qui signifie que* u *laisse stable toute droite de* E *et c'est une homothétie.*
On a donc $Z(\mathcal{L}(E)) = \mathbb{K} \cdot Id$.

(b) Pour $\dim(E) = 1$, *on a* $Z(GL(E)) = GL(E) = \mathbb{K}^* \cdot Id$.
On suppose E *est de dimension finie ou infinie au moins égale à* 2 *et on se donne* $u \in Z(GL(E))$.
Pour montrer que u *est une homothétie, il nous suffit de montrer que* u *laisse stable tout hyperplan de* E.
Si $H = \ker(\varphi)$, *où* $\varphi \in E^* \setminus \{0\}$ *est un hyperplan de* E, *on a alors* $E = \mathbb{K}a \oplus H$ *où* $a \in E$ *est tel que* $\varphi(a) \neq 0$.
On se donne $b \in H \setminus \{0\}$, *on se donne une base* $\mathcal{B}_H$ *de* H *et on définit* $v \in \mathcal{L}(E)$ *par :*

$$ \begin{cases} v(a) = a + b \\ \forall e \in \mathcal{B}_H,\ v(e) = e \end{cases} $$

de sorte que $v \in GL(E)$ *(son inverse est défini par* $v^{-1}(a) = a - b$ *et* $v^{-1}(e) = e$ *pour tout* $e \in \mathcal{B}_H$*) et* $H = \ker(v - Id)$. *Comme* u *commute à* v, *l'hyperplan* H *est stable par* u *(pour* $h \in H$, *on a* $(v - Id)(u(h)) = u((v - Id)(h)) = 0$, *donc* $u(h) \in \ker(v - Id) = H$*).*
Donc $u \in GL(E)$ *laisse stable tout hyperplan de* E *et c'est une homothétie de rapport non nul.*
On a donc $Z(GL(E)) = \mathbb{K}^* Id$.

Exercice 1.5 *Les groupes* $GL_n(\mathbb{Q})$, $GL_n(\mathbb{R})$ *et* $GL_n(\mathbb{C})$ *peuvent-ils être isomorphes ?*

Solution 1.5 *Si* $\mathbb{K}, \mathbb{L}$ *sont deux corps et* $\varphi : GL_n(\mathbb{K}) \to GL_n(\mathbb{L})$ *est un isomorphisme de groupes multiplicatifs, il induit alors un isomorphisme de* $Z(GL_n(\mathbb{K})) = \mathbb{K}^* I_n$ *sur* $Z(GL_n(\mathbb{L})) = \mathbb{L}^* I_n$, *ce qui induit un isomorphisme de groupes de* $\mathbb{K}^*$ *sur* $\mathbb{L}^*$.
Comme $\mathbb{Q}^*$ *est dénombrable, il ne peut être en bijection avec* $\mathbb{R}^*$ *[resp.* $\mathbb{C}^*$*] qui ne l'est pas.*
Comme i *est d'ordre* 4 *dans* $\mathbb{C}^*$ *et il n'y a pas d'élément d'ordre* 4 *dans* $\mathbb{R}^*$, *les groupes* $\mathbb{R}^*$ *et* $\mathbb{C}^*$ *ne peuvent être isomorphes.*

On peut vérifier que $GL_n(\mathbb{K})$ est produit semi-direct de $SL_n(\mathbb{K})$ et $\mathbb{K}^*$ (voir [**?**]). Avec l'exercice qui suit on donne une condition suffisante pour que $GL_n(\mathbb{K})$ soit isomorphe au produit direct $SL_n(\mathbb{K}) \times \mathbb{K}^*$.

C'est le cas par exemple pour $\mathbb{K} = \mathbb{R}$ et n impair, ou pour $\mathbb{K} = \mathbb{F}_q$ et n premier avec $q-1$.

Exercice 1.6 *On suppose que $n \geq 2$.*

1. *On suppose que le morphisme de groupes :*

$$\begin{array}{rccc} \varphi_n : & \mathbb{K}^* & \to & \mathbb{K}^* \\ & \lambda & \mapsto & \lambda^n \end{array}$$

est un isomorphisme.

   (a) *Donner des exemples de telle situation.*

   (b) *Montrer que l'application :*

$$\begin{array}{rccc} \theta_n : & SL_n(\mathbb{K}) \times \mathbb{K}^* & \to & GL_n(\mathbb{K}) \\ & (S, \lambda) & \mapsto & \lambda S \end{array}$$

   est un isomorphisme de groupes.

2. *On suppose qu'il existe un sous-groupe G de $GL_n(\mathbb{K})$ tel que l'application :*

$$\begin{array}{rccc} \theta_n : & SL_n(\mathbb{K}) \times G & \to & GL_n(\mathbb{K}) \\ & (S, A) & \mapsto & SA \end{array}$$

soit un isomorphisme de groupes.

   (a) *Montrer que l'application $\det : G \to \mathbb{K}^*$ est un isomorphisme de groupes et que le groupe G est commutatif.*

   (b) *Montrer que $G = Z(GL_n(\mathbb{K}))$ et $GL_n(\mathbb{K})$ est isomorphe $SL_n(\mathbb{K}) \times \mathbb{K}^*$.*

Solution 1.6

1.

   (a) *Pour $\mathbb{K} = \mathbb{R}$, φ_n est un isomorphisme si, et seulement si, n est impair (pour $n = 2r+1$, la fonction $x \mapsto x^{2r+1}$ réalise une bijection de $\mathbb{R}$ sur $\mathbb{R}$ et pour n pair, on a $(-1)^n = 1$).*
   Pour $\mathbb{K} = \mathbb{F}_q$, φ_n est un isomorphisme si, et seulement si, $\ker(\varphi_n) = \mu_n(\mathbb{F}_q) = \{1\}$ (puisque $\mathbb{F}_q^*$ est fini), ce qui revient à dire que n premier avec $q-1$ puisque $\mu_n(\mathbb{F}_q) = \mu_{n \wedge (q-1)}(\mathbb{F}_q)$ est de cardinal $n \wedge (q-1)$ (exercice 1.19).

   (b) *L'application :*

$$\begin{array}{rccc} \theta_n : & SL_n(\mathbb{K}) \times \mathbb{K}^* & \to & GL_n(\mathbb{K}) \\ & (S, \lambda) & \mapsto & \lambda S \end{array}$$

   est un morphisme de groupes injectif.
   En effet, il est clair que c'est un morphisme de groupes et pour $(S, \lambda) \in \ker(\theta_n)$, on a $\lambda S = I_n$, donc $\lambda^n = \det(\lambda S) = 1$ et $\lambda \in \ker(\varphi_n)$, soit $\lambda = 1$ puisque que φ_n est injective, ce qui nous donne $S = I_n$.
   Comme φ_n est surjective, pour toute matrice $A \in GL_n(\mathbb{K})$, il existe un scalaire $\lambda \in \mathbb{K}^*$ tel que $\lambda^n = \det(A)$, donc la matrice $S = \dfrac{1}{\lambda} A$ est dans $SL_n(\mathbb{K})$ et $\theta_n(S, \lambda) = A$, ce qui nous donne la surjectivité de θ_n.
   On a donc $GL_n(\mathbb{K}) \backsimeq SL_n(\mathbb{K}) \times \mathbb{K}^* \backsimeq SL_n(\mathbb{K}) \times Z(GL_n(\mathbb{K}))$.
   Par exemple, $GL_{2r+1}(\mathbb{R})$ est isomorphe à $SL_n(\mathbb{R}) \times \mathbb{R}^*$.

2.

(a) L'application $\det : G \to \mathbb{K}^*$ *est un morphisme de groupes.*
Si $A \in \ker(\det) \cap G = SL_n(\mathbb{K}) \cap G$, *on a alors :*

$$\theta_n\left(A, A^{-1}\right) = I_n$$

donc $A = I_n$ *puisque* θ_n *est injective.*
Donc $\det : G \to \mathbb{K}^*$ *est injectif.*
Comme $\det : GL_n(\mathbb{K}) \to \mathbb{K}^*$ *est surjectif, pour tout* $\lambda \in \mathbb{K}^*$ *il existe une matrice* $B \in GL_n(\mathbb{K})$ *telle que* $\det(B) = \lambda$ *et comme* θ_n *est surjectif, il existe* $(S, A) \in SL_n(\mathbb{K}) \times G$ *tel que* $SA = B$.
On a alors $\lambda = \det(B) = \det(S)\det(A) = \det(A)$.
Donc $\det : G \to \mathbb{K}^*$ *est surjectif et c'est un isomorphisme de groupes.*
Comme $\mathbb{K}^*$ *est commutatif, il en est de même de* G.

(b) Soit $A \in G$.
Pour toute matrice $B \in GL_n(\mathbb{K})$ *il existe un unique couple* $(S, A') \in SL_n(\mathbb{K}) \times G$ *tel que* $B = SA'$ *et comme* G *est commutatif, on a :*

$$\begin{aligned} AB &= (I_n A)(SA') = \theta_n(I_n, A)\,\theta_n(S, A') = \theta_n((I_n, A)(S, A')) \\ &= \theta_n(S, AA') = SAA' = SA'A = BA \end{aligned}$$

donc $A \in Z(GL_n(\mathbb{K}))$.
On a donc $G \subset Z(GL_n(\mathbb{K}))$.
Soit $A = \mu I_n \in \mathbb{K}^* I_n = Z(GL_n(\mathbb{K}))$.
Comme $\det : GL_n(\mathbb{K}) \to \mathbb{K}^*$ *et* $\theta_n : SL_n(\mathbb{K}) \times G \to GL_n(\mathbb{K})$ *sont surjectifs, il existe* $B \in GL_n(\mathbb{K})$ *et* $(S, A') \in SL_n(\mathbb{K}) \times G$ *tels que* $\det(B) = \mu$ *et* $B = SA'$. *La matrice* A' *étant dans* $G \subset Z(GL_n(\mathbb{K}))$, *elle s'écrit* $A' = \lambda I_n$ *et on a* $B = \lambda S$, *de sorte que* $\mu = \det(B) = \lambda^n \det(S) = \lambda^n$.
Il en résulte que $A = \mu I_n = \lambda^n I_n = (\lambda I_n)^n = (A')^n \in G$ *puisque* G *est un groupe.*
On a donc $Z(GL_n(\mathbb{K})) \subset G$ *et l'égalité* $G = Z(GL_n(\mathbb{K}))$.
L'application $\det : G = Z(GL_n(\mathbb{K})) \to \mathbb{K}^*$ *étant un isomorphisme de groupes, la composée :*

$$\lambda \in \mathbb{K}^* \mapsto \lambda I_n \in G \mapsto \det(\lambda I_n) = \lambda^n = \varphi_n(\lambda)$$

est un isomorphisme.
Réciproquement, si φ_n *est un isomorphisme, on a vu que pour* $H = Z(GL_n(\mathbb{K}))$, *l'application* θ_n *est un isomorphisme.*
On a donc montré que : $\varphi_n : \lambda \in \mathbb{K}^* \mapsto \lambda^n$ *est un isomorphisme si, et seulement si, il existe un sous-groupe* G *de* $GL_n(\mathbb{K})$ *tel que* $\theta_n : (S, A) \in SL_n(\mathbb{K}) \times G \mapsto SA \in GL_n(\mathbb{K})$ *est un isomorphisme.*

Exercice 1.7 *Montrer que :*

$$Z(GL(E)) = \{u \in GL(E) \mid \forall v \in GL(E),\ \exists \lambda \in \mathbb{K}^* \text{ tel que } u \circ v = \lambda \cdot v \circ u\}$$

Solution 1.7 *Il est équivalent de montrer que :*

$$Z(GL_n(\mathbb{K})) = \{A \in GL_n(\mathbb{K}) \mid \forall B \in GL_n(\mathbb{K}),\ \exists \lambda \in \mathbb{K}^* \text{ tel que } AB = \lambda BA\}$$

On traite d'abord le cas où $n = 2$ *(pour* $n = 1$, *il n'y a rien à prouver).*
Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{K})$ *telle que* $AB = \lambda_B BA$ *pour toute matrice* $B \in GL_2(\mathbb{K})$ *(le*

scalaire λ dépend de B).
On a alors $\det(AB) = \lambda_B^2 \det(BA) = \lambda_B^2 \det(AB)$ *et en conséquence* $\lambda_B^2 = 1$ *(puisque* $AB \in GL_2(\mathbb{K})$*), donc* $\lambda_B = \pm 1$.
En caractéristique 2, *on a* $\lambda_B = 1$ *et c'est terminé.*
En caractéristique différente de 2, *pour* $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{K})$, *dans le cas où* $\lambda_B = -1$, *on a :*

$$AB = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = -BA = -\begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}$$

ce qui impose $c = -c$ *et* $c = 0$, $d = -d$ *et* $d = 0$, *ce qui contredit le fait que* A *est inversible, on a donc* $\lambda_B = 1$, *soit :*

$$\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}$$

donc $c = 0$ *et* $a = d$.
De manière analogue, en prenant $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in SL_2(\mathbb{K})$, *on aboutit à* $b = 0$ *et* $A \in \mathbb{K}^* \cdot I_2 = Z(GL_2(\mathbb{K}))$.
Pour $n \geq 3$, *en utilisant les matrices* $B = I_n + E_{ij} \in SL_n(\mathbb{K})$ *où* $1 \leq i \neq j \leq n$, *on a :*

$$A + AE_{ij} = \lambda_{ij} A + \lambda_{ij} E_{ij} A$$

En prenant l'image de e_j, *on a :*

$$\begin{aligned} Ae_j + AE_{ij}e_j = Ae_j + Ae_i &= \lambda_{ij} Ae_j + \lambda_{ij} E_{ij} \left(\sum_{k=1}^{n} a_{kj} e_k \right) \\ &= \lambda_{ij} Ae_j + \lambda_{ij} a_{jj} e_i \end{aligned}$$

soit :

$$(1 - \lambda_{ij}) Ae_j + Ae_i = \lambda_{ij} a_{jj} e_i$$

avec $a_{jj} \neq 0$ *puisque la famille* (Ae_j, Ae_i) *est libre (du fait que* $A \in GL_n(\mathbb{K})$*).*
En prenant l'image de e_k, *pour* $1 \leq k \neq j \leq n$, *on a :*

$$Ae_k = \lambda_{ij} Ae_k + \lambda_{ij} E_{ij} \left(\sum_{p=1}^{n} a_{pk} e_p \right) = \lambda_{ij} Ae_k + \lambda_{ij} a_{jk} e_i$$

soit :

$$(1 - \lambda_{ij}) Ae_k = \lambda_{ij} a_{jk} e_i$$

Pour $\lambda_{ij} \neq 1$, *on abouti à* $a_{jk} \neq 0$, *donc :*

$$(1 - \lambda_{ij}) Ae_j + Ae_i = \lambda_{ij} a_{jj} e_i = a_{jj} \frac{1 - \lambda_{ij}}{a_{jk}} Ae_k$$

ce qui contredit le fait que la famille (Ae_j, Ae_i, Ae_k) *est libre en prenant* k *différent de* i *(ce qui est possible pour* $n \geq 3$*).*
On a donc $\lambda_{ij} = 1$, *soit* $AE_{ij} = E_{ij}A$ *pour tous* $i \neq j$ *compris entre* 1 *et* n, *donc* A *est une matrice scalaire et* $A \in Z(GL_n(\mathbb{K}))$.
L'autre inclusion est évidente.

On note :

$$PGL(E) = \frac{GL(E)}{Z(GL(E))} = \frac{GL(E)}{\mathbb{K}^* \cdot Id}$$

et :

$$PSL(E) = \frac{SL(E)}{Z(SL(E))} = \frac{SL(E)}{\mu_n(\mathbb{K}) \cdot Id}$$

(groupes projectifs linéaires).

Dans le cadre matriciel, on note :

$$PGL_n(\mathbb{K}) = \frac{GL_n(\mathbb{K})}{Z(GL_n(\mathbb{K}))} = \frac{GL_n(\mathbb{K})}{\mathbb{K}^* \cdot I_n}$$

et :

$$PSL_n(\mathbb{K}) = \frac{SL_n(\mathbb{K})}{Z(SL_n(\mathbb{K}))} = \frac{SL_n(\mathbb{K})}{\mu_n(\mathbb{K}) \cdot I_n}$$

Comme le centre $Z(G)$ d'un groupe G est un sous-groupe distingué de G, ces quotients sont bien des groupes.

Théorème 1.5 *On a $Z(PGL(E)) = Z(PSL(E)) = \{\overline{Id}\}$ [resp. $Z(PGL_n(\mathbb{K})) = Z(PSL_n(\mathbb{K})) = \{\overline{I_n}\}$].*

Démonstration. Dire que $\overline{A} \in Z(PGL_n(\mathbb{K}))$ revient à dire que $\overline{AB} = \overline{BA}$ pour tout $\overline{B} \in PGL_n(\mathbb{K})$, ce qui équivaut à dire qu'il existe $\lambda_B \in \mathbb{K}^*$ tel que $AB = \lambda_B BA$, soit que $A \in Z(GL_n(\mathbb{K})) = \mathbb{K}^* \cdot I_n$ ou $\overline{A} = \overline{I_n}$.

On a donc $Z(PGL_n(\mathbb{K})) = \{\overline{I_n}\}$.

On a aussi prouvé que $Z(PSL_n(\mathbb{K})) = \{\overline{I_n}\}$. ∎

Théorème 1.6 *Pour $\mathbb{K}$ algébriquement clos, les groupes $PGL(E)$ et $PSL(E)$ [resp. $PGL_n(\mathbb{K})$ et $PSL_n(\mathbb{K})$] sont isomorphes.*

Démonstration. L'injection $i : SL_n(\mathbb{K}) \to GL_n(\mathbb{K})$ induit un morphisme de groupes injectif :

$$\overline{i} : PSL_n(\mathbb{K}) = \frac{SL_n(\mathbb{K})}{\mu_n(\mathbb{K}) \cdot I_n} \to PGL_n(\mathbb{K}) = \frac{GL_n(\mathbb{K})}{\mathbb{K}^* \cdot I_n}$$

Si $A \equiv B$ modulo $\mu_n(\mathbb{K}) \cdot I_n$, on a aussi $A \equiv B$ modulo $\mathbb{K}^* \cdot I_n$, donc $\overline{i}$ est bien défini.

Il est clair que $\overline{i}$ est un morphisme de groupes.

Si A dans $SL_n(\mathbb{K})$ est tel que $A \equiv I_n$ modulo $\mathbb{K}^* \cdot I_n$, on a alors $A = \lambda I_n$ avec $\lambda \in \mathbb{K}^*$ et $1 = \det(A) = \lambda^n$, donc $A \equiv I_n$ modulo $\mu_n(\mathbb{K}) \cdot I_n$.

Le morphisme $\overline{i}$ est donc injectif (que $\mathbb{K}$ soit algébriquement clos ou pas).

Pour $B \in GL_n(\mathbb{K})$, il existe $\lambda \in \mathbb{K}^*$ tel que $\det(B) = \lambda^n$ puisque $\mathbb{K}$ est algébriquement clos et $A = \frac{1}{\lambda} B \in SL_n(\mathbb{K})$ est telle que $A \equiv B$ modulo $\mathbb{K}^* \cdot I_n$.

Le morphisme $\overline{i}$ est donc surjectif et c'est un isomorphisme de $PSL_n(\mathbb{K})$ sur $PGL_n(\mathbb{K})$. ∎

On rappelle qu'un groupe G est dit d'exposant fini s'il existe un entier $m \geq 1$ tel que $g^m = 1$ pour tout $g \in G$, ce qui signifie que tous les éléments de G sont d'ordre fini divisant n.

Le théorème de Lagrange nous dit que tout groupe fini est d'exposant fini (si G est d'ordre $n \geq 1$, tout élément g de G a un ordre qui divise n, donc $g^n = 1$), la réciproque n'étant vraie en général.

Pour les sous-groupe de $GL(E)$ et $\mathbb{K}$ algébriquement clos de caractéristique nulle, le théorème de Burnside qui suit nous dit que la réciproque est vraie, c'est-à-dire qu'un sous-groupe de $GL(E)$ est fini si, et seulement si, il est d'exposant fini.

Avec l'exercice qui suit, on s'intéresse d'abord aux sous-groupes de $GL(E)$ d'ordre 2.

Exercice 1.8 *On suppose que le corps* $\mathbb{K}$ *est de caractéristique différente de* 2.

1. *Soit* G *un sous-groupe de* $GL(E)$ *non réduit à* $\{Id\}$ *d'exposant égal à* 2.
   (a) *Montrer que tous les éléments de* G *sont diagonalisables de valeurs propres dans* $\{-1,1\}$.
   (b) *Montrer que* G *est commutatif et fini de cardinal* 2^r *où* r *est un entier compris entre* 0 *et* n.
2. *Soient* E, F *deux* $\mathbb{K}$*-espaces vectoriels de dimensions respectives* $n \geq 1$ *et* $m \geq 1$.
   Montrer que ces espaces vectoriels sont isomorphes si, et seulement si, les groupes $GL(E)$ *et* $GL(F)$ *sont isomorphes.*
   Pour $\mathbb{K}$ *fini de caractéristique* 2, *c'est encore vrai (exercice 1.17).*
   Pour $\mathbb{K}$ *infini de caractéristique* 2, *c'est encore vrai (plus difficile, voir J. Fresnel, Algèbre des matrices, Hermann, exercice A.4.7.21.3).*

Solution 1.8

1.
   (a) *Tous les éléments de* $G \subset GL(E)$ *étant d'ordre inférieur ou égal à* 2, *ils sont annulés par le polynôme* X^2-1 *qui est scindé à racine simples puisque* $\mathbb{K}$ *est de caractéristique différente de* 2, *donc ils sont diagonalisables avec leurs valeurs propres dans* $\{-1,1\}$.
   (b) *Dire que tous les éléments d'un groupe* $(G,\cdot)$ *sont d'ordre au plus égal à* 2, *revient à dire que l'on a* $g^2 = 1$, *ou encore que* $g = g^{-1}$, *pour tout* $g \in G$.
   Dans ce cas, pour tous g_1, g_2 *dans* G, *on a* $g_1 g_2 = (g_1 g_2)^{-1} = g_2^{-1} g_1^{-1} = g_2 g_1$, *donc* G *est commutatif.*
   Comme $G \subset GL(E)$ *est commutatif avec tous ses éléments diagonalisables, ils sont simultanément diagonalisables.*
   Il existe donc une base $(e_i)_{1\leq i\leq n}$ *de* E *dans laquelle, la matrice de chaque endomorphisme* $u \in G$ *est de la forme :*

$$D = \begin{pmatrix} \varepsilon_1(u) & 0 & \cdots & 0 \\ 0 & \varepsilon_2(u) & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \varepsilon_n(u) \end{pmatrix}$$

   où $\varepsilon_k(u) \in \{-1,1\}$, *pour tout* k *compris entre* 1 *et* n.
   On en déduit alors que l'application :

$$u \longmapsto (\varepsilon_1(u), \varepsilon_2(u), \cdots, \varepsilon_n(u))$$

   réalise un isomorphisme de groupes de G *sur un sous-groupe de* $\{-1,1\}^n$.
   Le groupe multiplicatif $\{-1,1\}^n$ *étant d'ordre* 2^n *et l'ordre d'un sous-groupe divisant l'ordre du groupe, on déduit que* G *est fini d'ordre* 2^r *avec* $0 \leq r \leq n$.
   De manière plus générale, on peut montrer que si $(G,\cdot)$ *est un groupe fini dont tout les éléments sont d'ordre au plus égal à* 2, *il est alors commutatif et* $\operatorname{card}(G) = 2^p$ *(exercice* **??***).*
2. *Si* E, F *sont isomorphes, on a alors* $m = n$ *et* $GL(E)$, $GL(F)$ *sont isomorphes à* $GL_n(\mathbb{K})$, *donc* $GL(E)$ *est isomorphe à* $GL(F)$.
   Réciproquement, supposons qu'il existe un isomorphisme de groupes φ *de* $GL(E)$ *dans*

$GL(F)$.
On se donne une base $\mathcal{B} = (e_i)_{1\leq i\leq n}$ de E et H est le sous-ensemble de $GL(E)$ formé des automorphisme u tels que :

$$u(e_i) = \varepsilon_i e_i \ (1 \leq i \leq n,\ \varepsilon_i \in \{-1, 1\})$$

Il est clair que H est un sous-groupe commutatif de $GL(E)$ isomorphe au sous-groupe à 2^n éléments de $GL_n(\mathbb{K})$ formé des matrices diagonales de termes diagonaux dans $\{-1, 1\}$ (comme $\text{caract}(\mathbb{K}) \neq 2$, *on a $-1 \neq 1$ dans $\mathbb{K}$ et ce groupe a bien 2^n éléments).*
$\varphi(H)$ est alors un sous-groupe commutatif à 2^n éléments de $GL(F)$ avec $n \leq m$.
Comme E et F jouent des rôles symétriques, on a aussi $m \leq n$ et $m = n$. Il en résulte que E et F sont isomorphes.

Le théorème de Burnside qui suit nous donne deux caractérisations des sous-groupes finis de $GL(E)$ pour un corps $\mathbb{K}$ de caractéristique nulle et algébriquement clos.

Pour ce qui suit le corps $\mathbb{K}$ est supposé algébriquement clos et de caractéristique nulle

Lemme 1.2 *Si G est un sous-groupe fini de $GL(E)$, alors tous ses éléments sont diagonalisables et l'ensemble :*

$$\text{tr}(G) = \{\text{tr}(u) \mid u \in G\}$$

est fini.

Démonstration. Pour $\text{card}(G) = 1$, on a $G = \{Id\}$ et le résultat est évident.

Soit G un sous-groupe de $GL(E)$ de cardinal $m \geq 2$.

Le théorème de Lagrange nous dit que pour tout $u \in G$, on a $u^m = Id$, c'est-à-dire que tous les éléments de G sont annulés par le polynôme $P_m(X) = X^m - 1$.

Le corps $\mathbb{K}$ étant algébriquement clos, ce polynôme P_m est scindé dans $\mathbb{K}[X]$.

Le corps $\mathbb{K}$ étant de caractéristique nulle, le polynôme dérivé mX^{m-1} s'annule uniquement en 0, donc le polynôme P_m est scindé à racines dans $\mathbb{K}[X]$ et tous les éléments de G sont diagonalisables.

Les valeurs propres de tout $u \in G$ étant racines de $X^m - 1$, elles sont en nombre fini quand u décrit G et en conséquence, $\text{tr}(G)$ est fini. ■

Nous allons montrer que la réciproque du lemme précédent est vraie, puis que tout groupe G d'exposant fini dans $GL(E)$ a tous ses éléments diagonalisables, l'ensemble $\text{tr}(G)$ étant fini, ce qui prouvera le théorème de Burnside.

Pour ce faire nous utiliserons les lemmes suivants qui nous donnent une caractérisation des endomorphismes nilpotents en utilisant la trace.

Lemme 1.3 *Un endomorphisme $u \in \mathcal{L}(E)$ est nilpotent si, et seulement si, 0 est la seule valeur propre de u.*

Démonstration. Si $u \in \mathcal{L}(E)$ est nilpotent d'ordre $q \geq 1$, on a alors $u^{q-1} \neq 0$ et $u^q = 0$, donc le polynôme minimal de u est $\pi_u(X) = X^q$ et 0 est l'unique valeur propre de u.

Réciproquement si 0 est la seule valeur propre de u avec $\mathbb{K}$ algébriquement clos, le polynôme minimal de u est alors X^q avec $1 \leq q \leq n$ et u est nilpotent. ■

Lemme 1.4 *Un endomorphisme $u \in \mathcal{L}(E)$ est nilpotent si, et seulement si, $\text{Tr}\left(u^k\right) = 0$ pour tout k compris entre 1 et $n = \dim(E)$.*

Démonstration. Si $u \in \mathcal{L}(E)$ est nilpotent, il en est alors de même de u^k pour tout entier $k \geq 1$, donc 0 est l'unique valeur propre de u^k et $\mathrm{Tr}\left(u^k\right) = 0$.

Réciproquement soit $u \in \mathcal{L}(E)$ tel que $\mathrm{Tr}\left(u^k\right) = 0$ pour tout k compris entre 1 et n.

S'il existe des valeurs propres non nulles $\lambda_1, \cdots, \lambda_p$ d'ordres respectifs $\alpha_1, \cdots, \alpha_p$ avec p compris entre 1 et n, on a alors :

$$\mathrm{Tr}\left(u^k\right) = \sum_{j=1}^{p} \alpha_j \lambda_j^k = 0 \ \ (1 \leq k \leq p)$$

(comme $\mathbb{K}$ est algébriquement clos, il existe une base de E dans laquelle la matrice de u est triangulaire de diagonale $(0, \cdots, 0, \lambda_1, \cdots, \lambda_1, \cdots, \lambda_p, \cdots, \lambda_p)$ et dans cette base, la matrice de u^k est également triangulaire de diagonale $\left(0, \cdots, 0, \lambda_1^k, \cdots, \lambda_1^k, \cdots, \lambda_p^k, \cdots, \lambda_p^k\right)$).

La matrice de ce système de p équations aux p inconnues α_j est une matrice de type Vandermonde de déterminant :

$$\begin{vmatrix} \lambda_1 & \cdots & \lambda_p \\ \vdots & \ddots & \vdots \\ \lambda_1^p & \cdots & \lambda_p^p \end{vmatrix} = \prod_{j=1}^{p} \lambda_j \begin{vmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ \lambda_1^{p-1} & \cdots & \lambda_p^{p-1} \end{vmatrix} = \prod_{j=1}^{p} \lambda_j \prod_{1 \leq i < j \leq p-1} (\lambda_j - \lambda_i) \neq 0$$

ce qui entraîne que tous les α_j sont nuls. Mais on a alors une contradiction avec $\alpha_j \neq 0$ dans $\mathbb{K}$ qui est de caractéristique nulle.

En définitive 0 est la seule valeur propre de u et u est nilpotent. ∎

Le lemme précédent est en fait valable pour $\mathbb{K}$ de caractéristique nulle.

Exercice 1.9 *Pour $\mathbb{K}$ de caractéristique nulle, montrer qu'un endomorphisme $u \in \mathcal{L}(E)$ est nilpotent si, et seulement si, $\mathrm{Tr}\left(u^k\right) = 0$ pour tout k compris entre 1 et n.*

Solution 1.9 *Pour la condition nécessaire, il suffit de vérifier qu'un endomorphisme nilpotent est de trace nulle (pour tout entier $k \geq 1$, u^k est aussi nilpotent).*
Pour ce faire, on peut procéder par récurrence sur la dimension $n \geq 1$ de E.
Pour $n = 1$, l'unique endomorphisme nilpotent est l'endomorphisme nul et sa trace est nulle.
Supposons le résultat acquis pour les espaces vectoriels de dimension au plus égale à $n - 1 \geq 1$ et soit $u \in \mathcal{L}(E)$ nilpotent d'ordre $q \geq 1$ avec E de dimension $n \geq 2$.
Comme 0 est valeur propre de u, il existe un vecteur non nul e_1 dans le noyau de u et en complétant ce vecteur en une base $\mathcal{B}$ de E, la matrice de u dans cette base est de la forme $A = \begin{pmatrix} 0 & \alpha \\ 0 & B \end{pmatrix}$ où $\alpha \in \mathcal{M}_{1,n-1}(\mathbb{K})$ et $B \in \mathcal{M}_{n-1}(\mathbb{K})$.
Avec $A^{q+1} = \begin{pmatrix} 0 & \alpha B^q \\ 0 & B^{q+1} \end{pmatrix} = 0$, on déduit que B est nilpotente et en conséquence $\mathrm{Tr}(B) = 0$ (l'hypothèse de récurrence nous donne le résultat sur $\mathcal{M}_{n-1}(\mathbb{K})$), ce qui entraîne $\mathrm{Tr}(u) = \mathrm{Tr}(A) = \mathrm{Tr}(B) = 0$.
*On peut aussi utiliser le théorème de réduction des endomorphismes nilpotents (théorème **??**).*
Pour la réciproque, on procède encore par récurrence sur la dimension $n \geq 1$ de E.
Pour $n = 1$, on a $u(x) = \lambda x$, $\mathrm{tr}(u) = \lambda$ et le résultat est trivial.
Supposons le résultat acquis pour les espaces vectoriels de dimension au plus égale à $n - 1 \geq 1$ et soit $u \in \mathcal{L}(E)$ tel que $\mathrm{Tr}\left(u^k\right) = 0$ pour tout k compris entre 1 et $n = \dim(E) \geq 2$.
En désignant par $P_u(X) = \sum_{k=0}^{n} a_k X^k$ le polynôme caractéristique de u et en tenant compte de $P_u(u) = \sum_{k=0}^{n} a_k u^k = 0$ et $\mathrm{tr}\left(u^k\right) = 0$ pour $k = 1, \cdots, n$, on déduit que $\mathrm{tr}(P(u)) = n a_0 = 0$ et

$a_0 = \det(u) = 0$ *puisque* $\mathbb{K}$ *de caractéristique nulle.*
Donc 0 *est valeur propre de* u *et il existe une base* $\mathcal{B}$ *de* E, *dans laquelle la matrice de* u *est de la forme* $A = \begin{pmatrix} 0 & \alpha \\ 0 & B \end{pmatrix}$ *où* $\alpha \in \mathcal{M}_{1,n-1}(\mathbb{K})$ *et* $B \in \mathcal{M}_{n-1}(\mathbb{K})$.
Avec $A^k = \begin{pmatrix} 0 & \alpha B^{k-1} \\ 0 & B^k \end{pmatrix}$, *on déduit que* $\operatorname{tr}(B^k) = \operatorname{tr}(A^k) = \operatorname{tr}(u^k) = 0$ *pour tout* $k = 1, \cdots, n$ *et l'hypothèse de récurrence nous dit que* B *est nilpotente.*
Enfin, en notant p *l'indice de nilpotence de* B, *avec* $A^{p+1} = \begin{pmatrix} 0 & \alpha B^p \\ 0 & B^{p+1} \end{pmatrix} = 0$, *on déduit que* A *est nilpotente et il en est de même de* u.

Lemme 1.5 *Soient* G *un sous-groupe de* $GL(E)$, F *le sous-espace vectoriel de* $\mathcal{L}(E)$ *engendré par* G, $\mathcal{B} = (u_i)_{1 \leq i \leq p}$ *une base de* F *extraite de* G *et* φ *l'application :*

$$\begin{array}{rccc} \varphi : & G & \to & \mathbb{K}^p \\ & u & \mapsto & (\operatorname{tr}(u \circ u_1), \cdots, \operatorname{tr}(u \circ u_p)) \end{array}$$

Si u, v *dans* G *sont tels que* $\varphi(u) = \varphi(v)$, *l'endomorphisme* $u \circ v^{-1} - Id$ *est alors nilpotent.*
Dans le cas où tous les éléments de G *sont diagonalisables, l'application* φ *est injective.*

Démonstration. Si u, v dans G sont tels que $\varphi(u) = \varphi(v)$, on a alors $\operatorname{tr}((u - v) \circ u_j) = 0$ pour tout j compris entre 1 et p, ce qui revient à dire que $\operatorname{tr}((u - v) \circ w) = 0$ pour tout $w \in F$.

Il en résulte que $\operatorname{tr}((u \circ v^{-1} - Id) \circ v \circ w) = 0$ pour tout $w \in G$, ce qui revient à dire que que l'on a $\operatorname{tr}((u \circ v^{-1} - Id) \circ w) = 0$ pour tout $w \in G$ puisque l'application $w \mapsto v \circ w$ est une permutation de G.

On a donc $u \circ v^{-1} \in G$ (G est un groupe) et $\operatorname{tr}(u \circ v^{-1} \circ w) = \operatorname{tr}(w)$ pour tout $w \in G$, ce qui entraîne $\operatorname{tr}(u \circ v^{-1}) = \operatorname{tr}(Id) = n$ et par récurrence $\operatorname{tr}\left((u \circ v^{-1})^k\right) = n$ pour tout $k \geq 0$.

Il en résulte que, pour tout $r \geq 1$, on a :

$$\begin{aligned} \operatorname{tr}\left((u \circ v^{-1} - Id)^r\right) &= \sum_{k=0}^{r} \binom{r}{k} (-1)^{r-k} \operatorname{tr}\left((u \circ v^{-1})^k\right) \\ &= n \sum_{k=0}^{r} \binom{r}{k} (-1)^{r-k} = n(1-1)^r = 0 \end{aligned}$$

et en conséquence, $u \circ v^{-1} - Id$ est nilpotent.

Si tous les éléments de G sont diagonalisables, l'endomorphisme $u \circ v^{-1}$ qui est dans G est diagonalisable et il en est de même de $u \circ v^{-1} - Id$.

Cet endomorphisme est donc diagonalisable et nilpotent et en conséquence nul (sa seule valeur propre est 0).

On a donc $u \circ v^{-1} = Id$, soit $u = v$ et φ est injective. ∎

Théorème 1.7 (Burnside) *Soit* G *un sous-groupe de* $GL(E)$.
Les assertions suivantes sont équivalentes :

1. *G est fini ;*
2. *G est d'exposant fini ;*
3. *tous les éléments sont diagonalisables et* $\operatorname{tr}(G)$ *est fini.*

Démonstration.

(1) $\Rightarrow$ (2) Si le groupe G est fini, le théorème de Lagrange nous dit alors qu'il est d'exposant fini.

(2) $\Rightarrow$ (3) Si G est d'exposant fini, il existe alors un entier $m \geq 1$ tel que $u^m = Id$ pour tout $u \in G$ et tous les éléments de G sont diagonalisables du fait qu'ils sont annulés par le polynôme $X^m - 1$ qui est scindé à racines simples dans $\mathbb{K}$ algébriquement clos (pour $m = 1$ c'est clair et pour $m \geq 2$, le polynôme dérivé mX^{m-1} s'annule uniquement en 0 puisque $\mathbb{K}$ est de caractéristique nulle).
Les valeurs propres de tout $u \in G$ étant racines de $X^m - 1$, elles sont en nombre fini quand u décrit G.
Il en résulte que $\mathrm{tr}(G)$ est fini est fini.

(3) $\Rightarrow$ (1) Si G a tous ses éléments diagonalisables, le lemme précédent nous dit que G est en bijection avec le sous-ensemble $\varphi(G)$ de $\mathbb{K}^p$.

Si de plus $\mathrm{tr}(G)$ est fini, $\varphi(G)$ est alors une partie finie de $\mathbb{K}^p$ en bijection avec G, donc G est fini. ■

Pour G sous-groupe fini de $GL(E)$, en notant $\theta(u)$ l'ordre d'un élément u de G, l'exposant de G est l'entier $r = \max_{u \in G} \theta(u)$.

Dans le cas où G est commutatif et $\mathbb{K} = \mathbb{C}$, les éléments de G sont simultanément diagonalisables, leurs valeurs propres étant dans l'ensemble Γ_r des racines r-èmes de l'unité, donc il existe une base E dans laquelle la matrice de chaque $u \in G$ est de la forme :

$$D = \begin{pmatrix} \lambda_1(u) & 0 & \cdots & 0 \\ 0 & \lambda_2(u) & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \lambda_n(u) \end{pmatrix}$$

où $\lambda_k(u) \in \Gamma_r$, pour tout k compris entre 1 et n.

On en déduit alors que l'application :

$$u \longmapsto (\lambda_1(u), \lambda_2(u), \cdots, \lambda_n(u))$$

réalise un morphisme de groupes injectif de G dans Γ_r^n et G est isomorphe à un sous-groupe de Γ_r^n, il est donc d'ordre qui divise r^n.

1.3 Générateurs de $SL(E)$ et de $GL(E)$

E est un $\mathbb{K}$-espace vectoriel de dimension finie $n \geq 2$ et E^* est l'espace dual de E.

Définition 1.1 *Soit φ une forme linéaire non nulle sur E.*
On appelle transvection d'hyperplan $\ker(\varphi)$ *toute application linéaire $u \in \mathcal{L}(E)$ définie par :*

$$\forall x \in E,\ u(x) = x + \varphi(x)\, a \tag{1.1}$$

où $a \in \ker(\varphi)$.

Définition 1.2 *Soit φ une forme linéaire non nulle sur E.*
On appelle dilatation d'hyperplan $\ker(\varphi)$ *toute application linéaire $u \in GL(E)$ définie par :*

$$\forall x \in E,\ u(x) = x + \varphi(x)\, a \tag{1.2}$$

où $a \in E \setminus \ker(\varphi)$.

On notera $\tau_{\varphi,a} = Id + \varphi \cdot a$ une transvection définie par (1.1), où $\varphi \in E^* \setminus \{0\}$ et $a \in \ker(\varphi)$ et $\delta_{\varphi,a} = Id + \varphi \cdot a$ une dilatation définie par (1.2) où $\varphi \in E^* \setminus \{0\}$ et $a \notin \ker(\varphi)$.

Avec notre définition $Id = \tau_{\varphi,0}$ est une transvection (transvection triviale). C'est la définition prise par Ramis-Warusfel, mais pas celle de Perrin où l'identité n'est pas une transvection.

Théorème 1.8

1. *Une transvection est dans $GL(E)$.*
2. *Une dilatation $\delta_{\varphi,a}$ est dans $GL(E)$ si, et seulement si $\lambda = 1 + \varphi(a) \neq 0$.*

Démonstration.

1. L'égalité $\tau_{\varphi,a}(x) = 0$ entraîne $x = -\varphi(x)\, a \in \ker(\varphi)$, donc $x = \tau_{\varphi,a}(x) = 0$.
   On a donc $\ker(\tau_{\varphi,a}) = \{0\}$ et $\tau_{\varphi,a} \in GL(E)$.
2. Si $\delta_{\varphi,a} \in GL(E)$, comme $a \notin \ker(\varphi)$, on a $a \neq 0$ et $\delta_{\varphi,a}(a) = (1 + \varphi(a))\, a \neq 0$, donc $\lambda \neq 0$.
   Réciproquement, en supposant λ non nul, l'égalité $\delta_{\varphi,a}(x) = x + \varphi(x)\, a = 0$ entraîne $\varphi(x)(1 + \varphi(a)) = 0$, donc $\varphi(x) = 0$ et $x = 0$.
   On a donc $\ker(\delta_{\varphi,a}) = \{0\}$ et $\delta_{\varphi,a} \in GL(E)$.

■

Pour une dilatation $\delta_{\varphi,a}$ qui est dans $GL(E)$, le scalaire $\lambda = 1 + \varphi(a) \in \mathbb{K} \setminus \{0, 1\}$ est le rapport de la dilatation ($\lambda \neq 1$ puisque $\varphi(a) \neq 0$).

Pour $\mathbb{K}$ de caractéristique différente de 2 et $\lambda = -1$, on dit que $\delta_{\varphi,a}$ est une réflexion d'hyperplan $\ker(\varphi)$.

Si $u = \delta_{\varphi,a} = \delta_{\varphi',a'}$, on a alors $\varphi(x)\, a = \varphi'(x)\, a'$ pour tout $x \in E$, donc $\varphi'(a')\, a' = \varphi(a')\, a$ avec $\varphi'(a') \neq 0$, ce qui nous donne $a' = \dfrac{\varphi(a')}{\varphi'(a')} a$, avec $\varphi(a') \neq 0$ et $\varphi \cdot a = \varphi' \cdot a' = \varphi' \cdot \dfrac{\varphi(a')}{\varphi'(a')} a$, soit $\varphi' = \dfrac{\varphi'(a')}{\varphi(a')} \varphi$.

Il en résulte que :

$$\varphi'(a') = \varphi'\left(\frac{\varphi(a')}{\varphi'(a')} a\right) = \frac{\varphi(a')}{\varphi'(a')} \varphi'(a) = \frac{\varphi(a')}{\varphi'(a')} \frac{\varphi'(a')}{\varphi(a')} \varphi(a) = \varphi(a)$$

Le scalaire $\lambda = 1 + \varphi(a)$ ne dépend donc que de la dilatation u.

Avec les deux théorèmes qui suivent, on donne des définitions équivalentes des transvections et dilatations.

Théorème 1.9 *Pour $u \in \mathcal{L}(E) \setminus \{Id\}$, les assertions suivantes sont équivalentes.*

1. *u est une transvection.*
2. *Il existe un hyperplan H de E tel que $u_{|H} = Id_H$ et $\operatorname{Im}(u - Id) \subset H$.*
3. *Il existe une base de E dans laquelle la matrice de u est de la forme :*

$$T_n = \begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

(pour $n = 2$, $T_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$).

4. *Il existe une base dans laquelle la matrice de u est de la forme :*

$$T_{ij}(\lambda) = I_n + \lambda E_{ij}$$

avec $1 \leq i \neq j \leq n$ et $\lambda \in \mathbb{K}^*$.

5. $\operatorname{rg}(u - Id) = 1$ *et le polynôme caractéristique de u est $P_u(X) = (X-1)^n$.*

Démonstration.

(1) $\Rightarrow$ (2) Si $u = \tau_{\varphi,a} = Id + \varphi \cdot a$ (avec $\varphi \in E^* \setminus \{0\}$ et $a \in \ker(\varphi) \setminus \{0\}$) est une transvection d'hyperplan $H = \ker(\varphi)$, on a alors :

$$u_{|H} = Id_H + \varphi_{|H} \cdot a = Id_H$$

et $\operatorname{Im}(u - Id) = \operatorname{Im}(\varphi \cdot a) = \mathbb{K}a \subset H$ ($\varphi \in E^* \setminus \{0\}$ est de rang égal à 1, donc surjective).

(2) $\Rightarrow$ (3) Soit $u \in \mathcal{L}(E) \setminus \{Id\}$ pour lequel il existe un hyperplan $H = \ker(\varphi)$ (où $\varphi \in E^* \setminus \{0\}$) tel que $u_{|H} = Id_H$ et $\operatorname{Im}(u - Id) \subset H$.
Pour $e_n \notin H$, on a $E = H \oplus \mathbb{K}e_n$ et le vecteur $e_{n-1} = u(e_n) - e_n$ est dans H (puisque $\operatorname{Im}(u - Id) \subset H$) et non nul (sinon $u(e_n) = e_n$ et $u = Id$ puisque $u_{|H} = Id_H$), donc la famille (e_{n-1}, e_n) est libre.
Pour $n \geq 3$, on peut compléter cette famille libre (e_{n-1}, e_n) en une base $\mathcal{B} = (e_k)_{1 \leq k \leq n}$ de E dans laquelle la matrice de u est la matrice $T_n = \begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ (pour $n = 2$, la matrice de u dans (e_1, e_2) est $T_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$).

(3) $\Rightarrow$ (4) La matrice de u dans une base adaptée est $T_n = I_n + E_{n-1,n} = T_{n-1,n}(1)$.

(4) $\Rightarrow$ (5) Si la matrice de $u \neq Id$ dans une base adaptée est $T_{ij}(\lambda) = I_n + \lambda E_{ij}$ où $1 \leq i \neq j \leq n$ et $\lambda \in \mathbb{K}^*$, on a alors :

$$\operatorname{rg}(u - Id) = \operatorname{rg}(T_{ij}(\lambda) - I_n) = \operatorname{rg}(\lambda E_{ij}) = \operatorname{rg}(E_{ij}) = 1$$

et :

$$P_u(X) = \det(XI_n - T_{ij}(\lambda)) = \det((X-1)I_n - \lambda E_{ij}) = (X-1)^n$$

(5) $\Rightarrow$ (1) Soit $u \in \mathcal{L}(E) \setminus \{Id\}$ tel que $\operatorname{rg}(u - Id) = 1$ et $P_u(X) = (X-1)^n$.
Comme $\dim(\operatorname{Im}(u - Id)) = 1$, il existe $a \in E \setminus \{0\}$ tel que $\operatorname{Im}(u - Id) = \mathbb{K}a$, donc pour tout $x \in E$, il existe un unique scalaire $\varphi(x) \in \mathbb{K}$ tel que $u(x) - x = \varphi(x)\, a$.
L'application $\varphi : E \to \mathbb{K}$ ainsi définie est non nulle (puisque $u \neq Id$) et linéaire.
En effet, en notant $v = u - Id$, pour x, y dans E et $\lambda \in \mathbb{K}$, on a :

$$\begin{aligned} v(x + \lambda y) &= \varphi(x + \lambda y)\, a \\ &= v(x) + \lambda v(y) = (\varphi(x) + \lambda\varphi(y))\, a \end{aligned}$$

avec $a \neq 0$, donc $\varphi(x + \lambda y) = \varphi(x) + \lambda\varphi(y)$.
Si $a \notin \ker(\varphi)$, en complétant a par une base de $\ker(\varphi)$, la matrice de u dans cette base est :

$$\begin{pmatrix} I_{n-1} & 0 \\ 0 & 1 + \varphi(a) \end{pmatrix}$$

et $P_u(X) = (X-1)^{n-1}(X - (1 + \varphi(a)))$ avec $\varphi(a) \neq 0$, ce qui contredit l'hypothèse $P_u(X) = (X-1)^n$.
En conclusion u est la transvection $\tau_{\varphi,a}$.

■

Théorème 1.10 *Pour $u \in GL(E)$, les assertions suivantes sont équivalentes.*

1. *u est une dilatation de rapport λ.*
2. *Il existe un hyperplan H de E tel que $u_{|H} = Id_H$ et u est diagonalisable de valeurs propres 1 et $\lambda \in \mathbb{K} \setminus \{0,1\}$ (c'est-à-dire que $E = \ker(u - Id) \oplus \ker(u - \lambda Id)$).*
3. *Il existe une base de E dans laquelle la matrice de u est de la forme :*

$$D_n(\lambda) = \begin{pmatrix} I_{n-1} & 0 \\ 0 & \lambda \end{pmatrix} = I_n + (\lambda - 1) E_{n,n}$$

avec $\lambda = \det(u) \in \mathbb{K} \setminus \{0,1\}$.

Démonstration.

(1) $\Rightarrow$ (2) Soit $u = \delta_{\varphi,a} \in GL(E)$ une dilatation d'hyperplan $H = \ker(\varphi)$ avec $a \notin H$.
On a $\ker(u - Id) = \ker(\varphi \cdot a) = \ker(\varphi)$ puisque $a \in E \setminus H$ est non nul, donc 1 est une valeur propre de u d'espace propre associé $\ker(u - Id) = H$ et $u \neq Id$.
Avec $u(a) = (1 + \varphi(a))\, a$ et $a \neq 0$, on déduit que $\lambda = 1 + \varphi(a) \neq 1$ est valeur propre de u, l'espace propre associé étant $\mathbb{K}a$. ($u(x) = x + \varphi(x)\, a = (1 + \varphi(a))\, x$ équivaut à $x = \dfrac{\varphi(x)}{\varphi(a)} a$) et u est diagonalisable puisque $E = H \oplus \mathbb{K}a$.
Comme on a supposé que $u \in GL(E)$, la valeur propre λ est non nulle.

(2) $\Rightarrow$ (3) C'est clair.

(2) $\Rightarrow$ (3) Si $u \in GL(E)$ a pour matrice $D_n(\lambda)$ avec $\lambda \in \mathbb{K} \setminus \{0,1\}$ dans une base $\mathcal{B} = (e_k)_{1 \leq k \leq n}$, pour tout $x = \sum_{k=1}^{n} x_k e_k \in E$, on a :

$$u(x) = \sum_{k=1}^{n-1} x_k e_k + \lambda x_n e_n = x + \varphi(x)\, a$$

où $\varphi(x) = x_n$ et $a = (\lambda - 1)\, e_n \notin H = \ker(\varphi)$ puisque $\lambda \neq 1$ et u est la dilatation $\delta_{\varphi,a}$.

■

Les propriétés de base des transvections et dilatations sont résumées avec les deux théorèmes qui suivent.

Théorème 1.11

1. *Une transvection $\tau_{\varphi,a}$ est dans $SL(E)$, son inverse étant la transvection $\tau_{\varphi,-a}$, 1 est son unique valeur propre, l'espace propre associé étant $\ker(\varphi)$ si $u \neq Id$.*
2. *Pour toute transvection $\tau_{\varphi,a}$, $\tau_{\varphi,a}^2 = \tau_{\varphi,2a}$ est une transvection.*
3. *L'ensemble $T(H)$ des transvections d'hyperplan $H = \ker(\varphi)$ est un sous groupe commutatif de $GL(E)$ isomorphe au groupe additif $(H, +)$.*
4. *Le polynôme minimal d'une transvection $u \neq Id$ est $(X - 1)^2$.*
5. *Pour $\mathbb{K}$ infini, toute transvection différente de Id s'écrit comme produit de deux matrices diagonalisables inversibles.*
6. *Le conjugué dans $GL(E)$ d'une transvection est une transvection.*

7. *Pour $n \geq 3$, toutes les transvections différentes de Id sont conjuguées dans $SL(E)$.*

Démonstration.

1. On peut utiliser la caractérisation matricielle.
   Dans une base adaptée la matrice de la transvection $\tau_{\varphi,a} \neq Id$ est est $T_n = \begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ avec $e_{n-1} = a$.
   Cette matrice est inversible d'inverse :
   $$T_n^{-1} = \begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$
   matrice de $\tau_{\varphi,-a}$.
   On peut aussi le vérifier directement (valable en dimension infinie).
   Soit $u = \tau_{\varphi,a}$ une transvection d'hyperplan $\ker(\varphi)$.
   L'application linéaire $v = \tau_{\varphi,-a}$ est une transvection d'hyperplan $\ker(\varphi)$ (on a bien $-a \in \ker(\varphi)$) et pour tout $x \in E$, on a :
   $$\begin{aligned} v \circ u(x) &= v(x + \varphi(x) a) = v(x) + \varphi(x) v(a) \\ &= x - \varphi(x) a + \varphi(x)(a - \varphi(a) a) = x \end{aligned}$$
   ($\varphi(a) = 0$ puisque $a \in \ker(\varphi)$).
   De manière analogue, on vérifie que $u \circ v = Id$ (pour la dimension infinie).
   Donc $\tau_{\varphi,a} \in GL(E)$ et $(\tau_{\varphi,a})^{-1} = \tau_{\varphi,-a}$.
   Pour $a = 0$, on a $u = Id$ qui a pour unique valeur propre 1.
   Supposons $a \neq 0$.
   Pour tout $\mu \in \mathbb{K}$, l'équation $u(x) = \mu x$ équivaut à $(1 - \mu) x + \varphi(x) a = 0$.
   Pour $\mu = 1$, cela équivaut à $\varphi(x) = 0$, soit à $x \in \ker(\varphi)$., donc 1 est valeur propre de u d'espace propre associé $\ker(\varphi)$.
   Pour $\mu \neq 1$, cela équivaut à $x = \dfrac{\varphi(x)}{\mu - 1} a \in \ker(\varphi)$, donc $\varphi(x) = 0$ et $x = 0$. La seule valeur propre de u est bien 1.
2. Si $\tau_{\varphi,a} = Id$, alors $\tau_{\varphi,a}^2 = Id$ est aussi une transvection.
   Pour tout $x \in E$, on a :
   $$\begin{aligned} \tau_{\varphi,a}^2(x) &= \tau_{\varphi,a}(x + \varphi(x) a) = x + \varphi(x) a + (\varphi(x) + \varphi(x)\varphi(a)) a \\ &= x + \varphi(x)(2a) = \tau_{\varphi,2a}(x) \end{aligned}$$
   (on a $\varphi(a) = 0$), donc $\tau_{\varphi,a}^2 = \tau_{\varphi,2a}$ est une transvection.
3. L'identité est la transvection $\tau_{\varphi,0}$, donc $T(H) \neq \emptyset$.
   Pour tout $a \in H$, on a vu que l'inverse de la transvection $\tau_{\varphi,a}$ est la transvection $\tau_{\varphi,-a} \in T(H)$.
   Pour a, b dans H et $x \in E$, on a :
   $$\begin{aligned} \tau_{\varphi,a} \circ \tau_{\varphi,b}(x) &= \tau_{\varphi,a}(x + \varphi(x) b) = \tau_{\varphi,a}(x) + \varphi(x) \tau_{\varphi,a}(b) \\ &= x + \varphi(x) a + \varphi(x)(b + \varphi(b) a) = x + \varphi(x)(a + b) \end{aligned}$$
   ($\varphi(b) = 0$) donc $\tau_{\varphi,a} \circ \tau_{\varphi,b} = \tau_{\varphi,a+b} = \tau_{\varphi,b+a} \in T(H)$.
   L'application $a \in H \mapsto \tau_{\varphi,a} \in T(H)$ réalise un isomorphisme de groupes de $(H, +)$ sur $(T(H), \circ)$ (c'est un morphisme de groupes surjectif et $\tau_{\varphi,a} = Id$ équivaut à $a = 0$).

4. Si $u = Id$, son polynôme minimal est $X - 1$.
   Si $u = \tau_{\varphi,a} \neq Id$, on a $u - Id = \varphi \cdot a \neq 0$ et pour tout $x \in E$:
   $$(u - Id)^2(x) = (u - Id)(\varphi(x)\, a) = \varphi(x)(u - Id)(a) = 0$$
   puisque $a \in \ker(\varphi) = \ker(u - Id)$. Donc le polynôme minimal est $(X-1)^2$.
5. Soit $u \in GL(E) \setminus \{Id\}$ une transvection de matrice :
   $$T_n = \begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$
   dans une base adaptée $\mathcal{B}$ de E.
   En désignant par v l'isomorphisme de E dont la matrice dans $\mathcal{B}$ est :
   $$D = \begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix}$$
   avec $\lambda_1 \neq \lambda_2$ dans $\mathbb{K}^*$ ($\mathbb{K}$ a au moins 3 éléments), la matrice dans $\mathcal{B}$ de l'isomorphisme $w = v \circ u$:
   $$\Delta = \begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & \lambda_1 & \lambda_1 \\ 0 & 0 & \lambda_2 \end{pmatrix}$$
   est diagonalisable (puisque $\begin{pmatrix} \lambda_1 & \lambda_1 \\ 0 & \lambda_2 \end{pmatrix}$ qui a deux valeurs propres distinctes l'est) et $u = v^{-1} \circ w$ est produit de deux matrices diagonalisables inversibles.
6. Soient $u = \tau_{\varphi,a}$ une transvection et $v \in GL(E)$.
   Pour tout $x \in E$, on a :
   $$\begin{aligned} v^{-1} \circ \tau_{\varphi,a} \circ v(x) &= v^{-1}(v(x) + (\varphi \circ v)(x)\, a) \\ &= x + (\varphi \circ v)(x)\, v^{-1}(a) = \tau_{\varphi \circ v, v^{-1}(a)}(x) \end{aligned}$$
   (on a bien $v^{-1}(a) \in \ker(\varphi \circ v)$ puisque $(\varphi \circ v)(v^{-1}(a)) = \varphi(a) = 0$).
   Donc :
   $$\forall v \in GL(E),\ v^{-1} \circ \tau_{\varphi,a} \circ v = \tau_{\varphi \circ v, v^{-1}(a)}$$
7. On suppose que $n \geq 3$.
   Si u, u' sont deux transvections différentes de Id, on peut alors trouver des bases $\mathcal{B} = (e_k)_{1 \leq k \leq n}$ et $\mathcal{B}' = (e'_k)_{1 \leq k \leq n}$ de E telles que $Mat_{\mathcal{B}}(u) = Mat_{\mathcal{B}'}(u') = T_n$.
   En désignant par v l'isomorphisme de E défini par $v(e_k) = e'_k$ pour tout k compris entre 1 et n, on a :
   $$v \circ u \circ v^{-1}(e'_k) = v \circ u(e_k) = v(e_k) = e'_k = u'(e'_k)\ \ (1 \leq k \leq n-1)$$
   et :
   $$v \circ u \circ v^{-1}(e'_n) = v \circ u(e_n) = v(e_{n-1} + e_n) = e'_{n-1} + e'_n = u'(e'_n)$$
   soit $u' = v \circ u \circ v^{-1}$.
   Donc u et u' sont conjuguées dans $GL(E)$ (on peut aussi simplement dire que u et u' ont

la même réduction de Jordan).

Si on peut trouver $w \in GL(E)$ tel que $w \circ u \circ w^{-1} = u$ et $\det(w) = \dfrac{1}{\det(v)}$, on aura :

$$\begin{aligned} u' = v \circ u \circ v^{-1} &= v \circ w \circ u \circ w^{-1} \circ v^{-1} \\ &= (v \circ w) \circ u \circ (v \circ w)^{-1} \end{aligned}$$

avec $\det(v \circ w) = 1$, soit $v \circ w \in SL(E)$, de sorte que u et u' seront conjuguées dans $SL(E)$.

Pour $n \geq 3$, en notant $\delta = \det(v)$, on peut définir w par :

$$Mat_{\mathcal{B}}(w) = \begin{pmatrix} I_{n-3} & 0 & 0 & 0 \\ 0 & \delta & 0 & 0 \\ 0 & 0 & \frac{1}{\delta} & 0 \\ 0 & 0 & 0 & \frac{1}{\delta} \end{pmatrix}$$

et on a :

$$\begin{aligned} Mat_{\mathcal{B}}\left(w \circ u \circ w^{-1}\right) &= \begin{pmatrix} I_{n-3} & 0 & 0 & 0 \\ 0 & \delta & 0 & 0 \\ 0 & 0 & \frac{1}{\delta} & 0 \\ 0 & 0 & 0 & \frac{1}{\delta} \end{pmatrix} \begin{pmatrix} I_{n-3} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} I_{n-3} & 0 & 0 & 0 \\ 0 & \frac{1}{\delta} & 0 & 0 \\ 0 & 0 & \delta & 0 \\ 0 & 0 & 0 & \delta \end{pmatrix} \\ &= \begin{pmatrix} I_{n-3} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = Mat_{\mathcal{B}}(u) \end{aligned}$$

donc $w \circ u \circ w^{-1} = u$ avec $\det(w) = \dfrac{1}{\delta}$.

■

Pour $n = 2$, les transvections différentes de Id sont toutes conjuguées dans $GL(E)$, mais pas dans $SL(E)$.

Si $u = \tau_{\varphi,a}$ est une transvection d'hyperplan $\ker(\varphi) = \mathbb{K}e_1$ avec $a = \alpha e_1 \in \ker(\varphi) \setminus \{0\}$, en prenant $e_2 \in E$ tel que $\mathcal{B} = (e_1, e_2)$ soit une base de E, on a $u(e_1) = e_1$ et $u(e_2) = e_2 + \varphi(e_2)\alpha e_1 = \lambda e_1 + e_2$, de sorte que la matrice de u dans $\mathcal{B}$ est :

$$A_\lambda = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

avec $\lambda \in \mathbb{K}^*$.

Si $u' = \tau_{\varphi',a'}$ est une autre transvection différente de Id telle que $\ker(\varphi') = \mathbb{K}e_2$, la matrices de u' dans la base $\mathcal{B}$ est :

$$B_\mu = \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}$$

avec μ dans $\mathbb{K}^*$.

Dire que ces transvections sont conjuguées dans $SL(E)$ signifie qu'il existe une matrice $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telle que $\det(P) = ad - bc = 1$ et $A_\lambda P = P B_\mu$, soit :

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}$$

ou encore :

$$\begin{pmatrix} a+c\lambda & b+d\lambda \\ c & d \end{pmatrix} = \begin{pmatrix} a+b\mu & b \\ c+d\mu & d \end{pmatrix}$$

donc :

$$\begin{cases} ad-bc=1 \\ c\lambda = b\mu \\ d\lambda = 0 \\ d\mu = 0 \end{cases} \Leftrightarrow \begin{cases} -bc=1 \\ c\lambda = b\mu \\ d=0 \end{cases} \Leftrightarrow \begin{cases} d=0,\ b\neq 0,\ c=-\dfrac{1}{b} \\ -\dfrac{\lambda}{\mu} = b^2 \end{cases}$$

On en déduit que si $-\dfrac{\lambda}{\mu}$ n'est pas un carré dans $\mathbb{K}^*$, les transvections u et u' ne peuvent être conjuguées dans $SL(E)$.

Pour $-\dfrac{\lambda}{\mu} = b^2$, prenant $c=-\dfrac{1}{b}$, $a=d=0$, on a :

$$\begin{aligned} P^{-1}A_\lambda P &= \begin{pmatrix} 0 & -b \\ \frac{1}{b} & 0 \end{pmatrix}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & b \\ -\frac{1}{b} & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ -\dfrac{1}{b^2}\lambda & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} = B_\mu \end{aligned}$$

Donc u et u' sont conjuguées dans $SL(E)$ si, et seulement si, $-\dfrac{\lambda}{\mu}$ est un carré dans $\mathbb{K}^*$.

Théorème 1.12

1. *L'inverse d'une dilatation de rapport λ est une dilatation de rapport $\dfrac{1}{\lambda}$.*
2. *Le polynôme minimal d'une dilatation de rapport λ est $(X-1)(X-\lambda)$.*
3. *Le conjugué dans $GL(E)$ d'une dilatation est une dilatation de même rapport.*
4. *Deux dilatations sont conjuguées dans $GL(E)$ si, et seulement si, elles ont même rapport.*

Démonstration.

1. C'est clair avec les matrices.
2. Si $u=\delta_{\varphi,a}$, on a alors pour tout $x\in E$:

$$(u-\lambda Id)\circ(u-Id)(x) = (u-\lambda Id)(\varphi(x)\,a) = \varphi(x)(u-\lambda Id)(a) = 0$$

   puisque $a\in\ker(u-\lambda Id)$.
   Comme $u-Id=\varphi\cdot a\neq 0$ et pour tout $h\in H\setminus\{0\}$, $(u-\lambda Id)(h)=(1-\lambda)h\neq 0$ puisque $\lambda\neq 1$, le polynôme minimal est $(X-1)(X-\lambda)$.
3. Soient $u=\delta_{\varphi,a}$ une dilatation et $v\in GL(E)$.
   Pour tout $x\in E$, on a :

$$\begin{aligned} v^{-1}\circ\delta_{\varphi,a}\circ v(x) &= v^{-1}(v(x)+(\varphi\circ v)(x)\,a) \\ &= x+(\varphi\circ v)(x)\,v^{-1}(a) = \delta_{\varphi\circ v, v^{-1}(a)} \end{aligned}$$

   (on a bien $v^{-1}(a)\notin\ker(\varphi\circ v)$ puisque $(\varphi\circ v)(v^{-1}(a))=\varphi(a)\neq 0$).
   Avec :

$$\varphi\circ v\left(v^{-1}(a)\right) = \varphi(a)$$

   on déduit que $v^{-1}\circ\delta_{\varphi,a}\circ v=\delta_{\varphi\circ v,v^{-1}(a)}$ a même rapport $\lambda=1+\varphi(a)$ que $u=\delta_{\varphi,a}$.

4. On a déjà vu que le conjugué dans $GL(E)$ d'une dilatation est une dilatation de même rapport.
   Réciproquement, deux dilatations de même rapport ont même représentation matricielle dans des bases adaptées, donc elles sont conjuguées.

■

On peut utiliser le polynôme minimal $\pi_u(X) = (X-1)(X-\lambda)$ d'une dilatation pour calculer u^{-1}.

De $u^2 - (1+\lambda)u + \lambda Id = 0$, on déduit que :

$$\begin{aligned} u^{-1} &= -\frac{1}{\lambda}(u - (1+\lambda)Id) = -\frac{1}{\lambda}(\varphi \cdot a - \lambda Id) \\ &= Id - \frac{1}{\lambda}\varphi \cdot a = \delta_{-\frac{\varphi}{\lambda},a} \end{aligned}$$

et u^{-1} est une dilatation de rapport $1 - \dfrac{\varphi(a)}{\lambda} = 1 - \dfrac{\lambda - 1}{\lambda} = \dfrac{1}{\lambda}$.

Les lemmes qui suivent nous seront utiles pour montrer que le groupe $SL(E)$ est engendré par l'ensemble des transvections.

Lemme 1.6 *Soient H_1, H_2 deux hyperplans distincts de E et $a \in E \setminus (H_1 \cup H_2)$.*

1. *L'ensemble $H = H_1 \cap H_2 \oplus \mathbb{K}a$ est un hyperplan de E.*
2. *On a $E = H + H_1 = H + H_2$.*
3. *Il existe une transvection u telle que $u(a) = a$ et $u(H_1) = H_2$.*

Démonstration.

1. On a $H_1 = \ker(\varphi_1)$ et $H_2 = \ker(\varphi_2)$ avec φ_1, φ_2 non colinéaires dans E^*.
   L'application $x \in E \mapsto (\varphi_1(x), \varphi_2(x)) \in \mathbb{K}^2$ est alors de rang 2 et son noyau $H_1 \cap H_2$ est un sous-espace de E de dimension $n-2$.
   Comme $a \in E \setminus (H_1 \cup H_2)$, on a $(H_1 \cap H_2) \cap \mathbb{K}a = \{0\}$ et le sous-espace vectoriel $H = H_1 \cap H_2 \oplus \mathbb{K}a$ est un hyperplan de E.
2. Pour $k = 1, 2$, on a :
   $$\dim(H + H_k) = \dim(H) + \dim(H_k) - \dim(H \cap H_k)$$
   avec $H \cap H_k = H_1 \cap H_2$ ($x \in H \cap H_k$ s'écrit $x = h + \lambda a$ avec $h \in H_1 \cap H_2$ et $\lambda \neq 0$ donne $a = \dfrac{1}{\lambda}(x - h) \in H_k$, ce qui contredit $a \in E \setminus (H_1 \cup H_2)$), donc :
   $$\begin{aligned} \dim(H + H_k) &= \dim(H) + \dim(H_k) - \dim(H_1 \cap H_2) \\ &= 2(n-1) - (n-2) = n \end{aligned}$$
   et $H + H_k = E$.
3. Si, pour $k = 1, 2$, $H_k \subset H$, on a alors $H = H_k$ à cause des dimensions et $a \in H_k$, ce qui contredit $a \in E \setminus (H_1 \cup H_2)$.
   On peut donc trouver $a_2 \in H_2 \setminus H$ et un tel élément s'écrit $a_2 = a_1 + b$ avec $a_1 \in H_1 \setminus H$ et $b \in H$ ($E = H + H_1$).
   Comme $a_1 \in H_1 \setminus H$, on a $a_1 \in H_1 \setminus H_1 \cap H_2$ et $H_1 = H_1 \cap H_2 \oplus \mathbb{K}a_1$.
   Comme $a_1 \in H_1 \setminus H$, on peut trouver une équation φ de H telle que $\varphi(a_1) = 1$ et en désignant par u la transvection $\tau_{\varphi,b}$, on a :
   $$u(a) = a + \varphi(a)\, b = a$$

puisque $a \in H$ et :

$$u(a_1) = a_1 + \varphi(a_1) b = a_1 + b = a_2 \in H_2$$

avec :

$$\forall x \in H_1 \cap H_2,\ u(x) = x + \varphi(x) b = x \in H_2$$

puisque $H_1 \cap H_2 \subset H$.
On en déduit que $u(H_1) \subset H_2$ (puisque $H_1 = H_1 \cap H_2 \oplus \mathbb{K}a_1$) et l'égalité $u(H_1) = H_2$ du fait que H_1 et H_2 sont de même dimension et u est un isomorphisme.

■

Lemme 1.7 *Pour tous x, y non nuls dans E, il existe $u \in SL(E)$ produit de une ou deux transvections tel que $y = u(x)$.*

Démonstration. Si x, y sont non colinéaires, en notant $a = y - x$, on peut trouver une forme linéaire non nulle φ telle que $\varphi(a) = 0$, $\varphi(x) = 1$ et en désignant par u la transvection $\tau_{\varphi, y-x}$, on a $u(x) = x + \varphi(x)(y - x) = y$.

Pour x, y colinéaires, on choisit z non colinéaire à x (et à y), ce qui est possible puisque $n \geq 2$ et on peut trouver deux transvections u, v telles que $u(x) = z$, $v(z) = y$, ce qui nous donne $v \circ u(x) = y$. ■

Théorème 1.13 *Le groupe $SL(E)$ est engendré par l'ensemble des transvections.*

Démonstration. On procède par récurrence sur $n \geq 2$.

Pour $n = 2$, soient $u \in SL(E)$ et $e_1 \in E \setminus \{0\}$.

On peut trouver $v \in SL(E)$ produit de une ou deux transvections tel que $u(e_1) = v(e_1)$, ce qui nous donne $v^{-1} \circ u(e_1) = e_1$ et complétant e_1 en une base (e_1, e_2) de E, la matrice de $v^{-1} \circ u$ dans cette base est $A = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ ($\det(A) = 1$), ce qui est la matrice d'une transvection.

Comme l'inverse d'une matrice de transvection est une matrice de transvection, on déduit que u est produit de une, deux ou trois transvections.

Supposons le résultat acquis pour les espaces vectoriels de dimension $n-1 \geq 2$ et soit $u \in SL(E)$ où $\dim(E) = n$.

Pour $a \in E \setminus \{0\}$, on peut trouver $v_1 \in SL(E)$ produit de une ou deux transvections tel que $u(a) = v_1(a)$, ce qui nous donne $v_1^{-1} \circ u(a) = a$ avec $v_2 = v_1^{-1} \circ u \in SL(E)$.

On se donne un hyperplan H_1 qui ne contient pas a (donc $E = H_1 \oplus \mathbb{K}a$) et H_2 est l'hyperplan $v_2(H_1)$.

Comme $v_2(a) = a$ avec v_2 bijective, on a $a \notin H_2$.

Si $H_1 \neq H_2$, il existe alors une transvection τ telle que $\tau(a) = a$ et $\tau(H_1) = H_2$.

En notant $v_3 = \tau^{-1} \circ v_2$, on a $v_3 \in SL(E)$, $H_1 = v_3(H_1)$ et $v_3(a) = \tau^{-1} \circ v_2(a) = a$.

La restriction de v_3 à H_1 est dans $SL(H_1)$, donc elle s'écrit comme produit de transpositions, $v_{3|H_1} = \prod_{k=1}^{p} \tau_k$.

En prolongeant les τ_k à E en posant $\tau_k(a) = a$, on définit des transpositions de E et $v_3 = \prod_{k=1}^{p} \tau_k$, ce qui nous donne $u = v_1 \circ \tau \circ v_3$ produit de transpositions. ■

Ce résultat peut aussi se montrer en utilisant les opérations élémentaires sur les matrices.

Corollaire 1.1 *Le groupe $GL(E)$ est engendré par l'ensemble des dilatations et des transvections.*

Démonstration. Soit $u \in GL(E) \backslash SL(E)$ de déterminant $\lambda \in \mathbb{K} \backslash \{0,1\}$ (pour $u \in SL(E)$, c'est déjà fait).

Pour toute dilatation $\delta_{\varphi,a}$ de rapport $\dfrac{1}{\lambda} \in \mathbb{K} \setminus \{0,1\}$, on a $v = \delta_{\varphi,a} \circ u \in SL(E)$, donc v est produit de transvections et $u = \delta_{\varphi,a}^{-1} \circ v = \delta_{-\lambda\varphi,a} \circ v$ est produit d'une dilatation et de transvections. ■

Exercice 1.10 *Montrer que, pour $\mathbb{K}$ ayant au moins trois éléments ($\mathbb{K} \neq \mathbb{F}_2$), le groupe $GL(E)$ est engendré par l'ensemble des dilatations.*

Solution 1.10 *Il suffit de montrer que toute transvection peut s'écrire comme produit de deux dilatations.*
Pour $\tau = Id$, c'est clair (l'inverse d'une dilatation est une dilatation).
Soit $\tau_{\varphi,a} \neq Id$ une transvection ($\varphi \in E^* \setminus \{0\}$ et $a \in \ker(\varphi)$, $a \neq 0$).
Pour toutes dilations δ_{φ_1,a_1} et δ_{φ_2,a_2} ($\varphi_k \in E^* \setminus \{0\}$ et $a_k \notin \ker(\varphi_k)$), l'égalité $\tau_{\varphi,a} = \delta_{\varphi_1,a_1} \circ \delta_{\varphi_2,a_2}$ équivaut à :

$$\begin{aligned} x + \varphi(x)\, a &= \delta_{\varphi_1,a_1}(x + \varphi_2(x)\, a_2) \\ &= x + \varphi_2(x)\, a_2 + \varphi_1(x + \varphi_2(x)\, a_2)\, a_1 \end{aligned}$$

pour tout $x \in E$.
Prenant φ_1, φ_2 telles que $\varphi_k(a) \neq 0$ (il faudra vérifier que c'est possible) et $a_1 = a_2 = a$, on doit avoir :

$$\varphi(x)\, a = (\varphi_2(x) + \varphi_1(x + \varphi_2(x)\, a))\, a$$

soit :

$$\varphi(x) = \varphi_1(x) + \varphi_2(x)\,(1 + \varphi_1(a))$$

Pour ce faire, on se donne $\varphi_1 \in E^* \setminus \{0\}$ telle que $\varphi_1(a) = 1 \notin \{-1, 0\}$ (c'est possible puisque $a \neq 0$ et $\mathbb{K} \neq \mathbb{F}_2$) et on définit φ_2 par :

$$\varphi_2(x) = \frac{\varphi(x) - \varphi_1(x)}{2}$$

(on a bien $\varphi_2(a) = \dfrac{\varphi(a) - \varphi_1(a)}{2} = -\dfrac{1}{2} \neq 0$).
Comme une matrice de dilatation est diagonalisable inversible, on retrouve le fait qu'une transvection est produit de deux matrices diagonalisables inversibles.

Exercice 1.11 *Montrer que, pour $\mathbb{K}$ infini, le groupe $GL(E)$ est engendré par l'ensemble des matrices diagonalisables inversibles.*

Solution 1.11 *Résulte du fait que $GL(E)$ est engendré par l'ensemble des dilatations, une matrice de dilatation étant diagonalisable inversible.*

Exercice 1.12 *Montrer que le groupe $GL(E)$ est engendré par l'ensemble $TN(E)$ des automorphismes de E de trace nulle.*
Indication : utiliser des matrices de permutation pour $n \geq 3$.

Solution 1.12 *On vérifie d'abord que toute transvection $\tau_{\varphi,a}$ peut s'écrire comme produit de deux éléments de $TN(E)$.*
Pour $n = 2$, la matrice de $\tau_{\varphi,a}$ dans une base adaptée est :

$$T_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

et pour $n \geq 3$, c'est :

$$T_n = \begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

En désignant par P_σ la matrice de permutation :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & 1 & \cdots & n-1 \end{pmatrix}$$

on a :

$$M = P_\sigma T_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \in TN(E)$$

et $T_n = P_\sigma^{-1} M = P_{\sigma^{-1}} M$ avec :

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & \cdots & n \\ 2 & 3 & \cdots & 1 \end{pmatrix}$$

soit :

$$P_{\sigma^{-1}} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \in TN(E)$$

On en déduit que tout élément de $SL(E)$ est produit d'éléments de $TN(E)$.
Soit $u \in GL(E) \setminus SL(E)$ de déterminant $\lambda \in \mathbb{K} \setminus \{0,1\}$.
On peut trouver $v \in TN(E)$ de déterminant λ. On peut prendre l'automorphisme de matrice :

$$M = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & (-1)^{n+1}\lambda \\ 1 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

dans une base de E.
On a alors $w = u \circ v^{-1} \in SL(E)$ qui est produit d'éléments de $TN(E)$ et il en est de même de $u = w \circ v$.

Exercice 1.13 *On suppose que le corps $\mathbb{K}$ est infini et on se donne un morphisme de groupes γ de $GL_n(\mathbb{K})$ dans $\mathbb{K}^*$ qui soit une fonction polynomiale des coefficients a_{ij} des matrices $A = ((a_{ij}))_{1 \leq i,j \leq n} \in GL_n(\mathbb{K})$.*

1. *Montrer qu'il existe un entier naturel r tel que pour toute matrice de la dilatation $D_n(\lambda) = \begin{pmatrix} I_{n-1} & 0 \\ 0 & \lambda \end{pmatrix}$ avec $\lambda \in \mathbb{F}_q^*$, on a $\gamma(D_n(\lambda)) = \lambda^r$.*

2. *Montrer que, pour toute matrice de transvection* $T_{ij}(\lambda) = I_n + \lambda E_{ij}$ *où* $1 \leq i \neq j \leq n$ *et* $\lambda \in \mathbb{F}_q$, *on a* $\gamma(T_{ij}(\lambda)) = 1$.
3. *Déduire de ce qui précède que :*

$$\forall A \in GL_n(\mathbb{K}),\ \gamma(A) = (\det(A))^r$$

Solution 1.13

1. *L'application :*

$$\varphi : \lambda \in \mathbb{K}^* \mapsto \gamma(D_n(\lambda)) \in \mathbb{K}^*$$

est un morphisme de groupes et une fonction polynomiale de λ.
Il existe donc un polynôme $P(X) = \sum_{k=0}^{r} \alpha_k X^k \in \mathbb{K}[X]$ *de degré* $r \geq 0$ *(donc avec* $\alpha_r \neq 0$*)* *tel que :*

$$\forall \lambda \in \mathbb{K}^*,\ \varphi(\lambda) = \sum_{k=0}^{r} \alpha_k \lambda^k$$

avec de plus la propriété :

$$\forall \lambda \in \mathbb{K}^*,\ \forall j \in \mathbb{N},\ \varphi\left(\lambda^j\right) = (\varphi(\lambda))^j$$

En désignant par p *la valuation du polynôme* p, *on a :*

$$\forall \lambda \in \mathbb{K}^*,\ \forall j \in \mathbb{N},\ \sum_{k=p}^{r} \alpha_k \lambda^{kj} = \left(\sum_{k=p}^{r} \alpha_k \lambda^k\right)^j$$

soit :

$$\forall \lambda \in \mathbb{K}^*,\ \forall j \in \mathbb{N},\ \sum_{k=p}^{r} \alpha_k \lambda^{(k-p)j} = \left(\sum_{k=p}^{r} \alpha_k \lambda^{k-p}\right)^j$$

ou encore :

$$\forall \lambda \in \mathbb{K}^*,\ \forall j \in \mathbb{N},\ \sum_{k=0}^{r-p} \alpha_{p+k} \lambda^{kj} = \left(\sum_{k=0}^{r-p} \alpha_{p+k} \lambda^k\right)^j$$

Comme le corps $\mathbb{K}$ *est infini, on en déduit les identités polynomiales :*

$$\forall j \in \mathbb{N},\ \sum_{k=0}^{r-p} \alpha_{p+k} X^{kj} = \left(\sum_{k=0}^{r-p} \alpha_{p+k} X^k\right)^j$$

Si $r-p \geq 1$, *en désignant par* q *le premier indice compris entre* 1 *et* $r-p$ *tel que* $\alpha_{p+q} \neq 0$, *on a :*

$$\alpha_p + \alpha_{p+q} X^{qj} + \cdots + \alpha_r X^{(r-p)j} = \left(\alpha_p + \alpha_{p+q} X^q + \cdots + \alpha_r X^{(r-p)}\right)^j$$

pour tout entier $j \geq 2$.
Dans le membre de gauche de cette identité, le coefficient de X^q *est nul et dans le terme de droite c'est* $j\alpha_p^{j-1}\alpha_{p+q}$, *donc :*

$$\forall j \geq 2,\ j\alpha_p^{j-1}\alpha_{p+q} = 0$$

avec α_p *et* α_{p+q} *non nuls, ce qui est impossible (pour* $\mathbb{K}$ *de caractéristique nulle c'est clair et pour* $\mathbb{K}$ *de caractéristique* $p' \geq 2$, *il suffit de prendre* j *non multiple de* p'*).*
On a donc $p = r$ *et :*

$$\forall \lambda \in \mathbb{K}^*,\ \varphi(\lambda) = \gamma(D_n(\lambda)) = \alpha_r \lambda^r$$

Pour $\lambda = 1$, *on a* $1 = \varphi(1) = \alpha_r$.

2. *Pour $1 \leq i \neq j \leq n$ fixés, l'application :*

$$\varphi : \lambda \in \mathbb{K} \mapsto \gamma\left(T_{ij}(\lambda)\right) \in \mathbb{K}^*$$

est un morphisme de groupes de $(\mathbb{K}, +)$ dans $(\mathbb{K}^*, \cdot)$.
En effet, pour λ, μ dans $\mathbb{K}$, on a $\varphi(\lambda+\mu) = \gamma\left(T_{ij}(\lambda+\mu)\right)$ avec :

$$\begin{aligned} T_{ij}(\lambda+\mu) &= I_n + (\lambda+\mu) E_{ij} = (I_n + \lambda E_{ij})(I_n + \mu E_{ij}) \\ &= T_{ij}(\lambda) T_{ij}(\mu) \end{aligned}$$

puisque $E_{ij}^2 = 0$ pour $i \neq j$, donc :

$$\begin{aligned} \varphi(\lambda+\mu) &= \gamma\left(T_{ij}(\lambda) T_{ij}(\mu)\right) = \gamma\left(T_{ij}(\lambda)\right)\gamma\left(T_{ij}(\mu)\right) \\ &= \varphi(\lambda)\varphi(\mu) \end{aligned}$$

De plus φ est une fonction polynomiale de λ.
Pour tout entier $k \geq 2$ et tout $\lambda \in \mathbb{K}$, on a $\varphi(k\lambda) = (\varphi(\lambda))^k$.
Prenant, pour $\mathbb{K}$ de caractéristique $p' \neq 0$, $k \geq 2$ non multiple de p, on en déduit l'identité polynomiale $\varphi(kX) = (\varphi(X))^k$ et $\deg(\varphi) = k\deg(\varphi)$, ce qui impose $\deg(\varphi) = 0$, ce qui signifie que φ est la fonction constante égale à $\varphi(0) = 1$ ou encore que $\gamma\left(T_{ij}(\lambda)\right) = 1$ pour tout $\lambda \in \mathbb{K}$.

3. *Résulte du fait que toute matrice $A \in GL_n(\mathbb{K})$ est produit de matrices de transvections (si elle est dans $SL_n(\mathbb{K})$) ou d'une matrice de dilatation de rapport $\det(A)$ et de matrices de transvections (si elle n'est pas dans $SL_n(\mathbb{K})$).*

1.4 Groupes dérivés de $GL(E)$ et de $SL(E)$

On rappelle le sous-groupe engendré par une partie non vide X d'un groupe $(G, \cdot)$ est l'intersection de tous les sous-groupes de G qui contiennent X. Il est noté $\langle X \rangle$ et on a :

$$\langle X \rangle = \left\{ \prod_{k=1}^{r} x_k^{\varepsilon_k} \mid r \in \mathbb{N}^*,\ x_k \in X \text{ et } \varepsilon_k \in \{-1, 1\} \text{ pour } 1 \leq k \leq r \right\}$$

Le groupe dérivé d'un groupe $(G, \cdot)$ est le sous-groupe $D(G)$ de G engendré par les commutateurs, c'est-à-dire les éléments de G de la forme :

$$[a, b] = aba^{-1}b^{-1}$$

où a, b sont dans G.

Deux éléments a, b de G commutent si, et seulement, on a $[a, b] = 1$ (d'où l'appellation commutateur).

Pour un groupe commutatif, on a $D(G) = \{1\}$.

L'inverse d'un commutateur est un commutateur. En effet, pour a, b dans G, on a :

$$[a, b]^{-1} = \left(aba^{-1}b^{-1}\right)^{-1} = bab^{-1}a^{-1} = [b, a]$$

Il en résulte que $D(G)$ est l'ensemble de tous les produits finis de commutateurs.

Exercice 1.14 *Montrer que $D(G)$ est le plus petit sous-groupe distingué de G tel que le groupe $\dfrac{D}{H}$ soit commutatif.*

Solution 1.14 *Le sous-groupe dérivé $D(G)$ est distingué dans G.*
En effet, pour a, b, c dans G, on a :

$$\begin{aligned} c[a,b]c^{-1} &= c\left(aba^{-1}b^{-1}\right)c^{-1} \\ &= \left(cac^{-1}\right)\left(cbc^{-1}\right)\left(ca^{-1}c^{-1}\right)\left(cb^{-1}c^{-1}\right) \\ &= \left[cac^{-1}, cbc^{-1}\right] \end{aligned}$$

Le groupe quotient $\dfrac{G}{D(G)}$ est commutatif.
En effet, pour a, b dans G, on a :

$$\begin{aligned} \overline{a}\overline{b} = \overline{ab} &= (ab)D(G) = (ba)\left(a^{-1}b^{1}ab\right)D(G) \\ &= (ba)\left[a^{-1}, b^{-1}\right]D(G) = (ba)D(G) = \overline{b}\overline{a} \end{aligned}$$

Soit H un sous-groupe distingué de G tel que le groupe $\dfrac{D}{H}$ soit commutatif.
Pour tous a, b dans G, on a $\overline{[a,b]} = \left[\overline{a}, \overline{b}\right] = \overline{1}$ dans le quotient $\dfrac{D}{H}$, ce qui revient à dire que $[a,b] \in H$. Le groupe H contient donc tous les commutateurs et en conséquence il contient le groupe dérivé $D(G)$.

Théorème 1.14

1. *On a $D(SL(E)) \subset D(GL(E)) \subset SL(E)$.*
2. *Pour $n \geq 3$, on a $D(SL(E)) = D(GL(E)) = SL(E)$.*
3. *Pour $n = 2$ et $\mathbb{K} \neq \mathbb{F}_2$, on a $D(GL(E)) = SL(E)$.*
4. *Pour $n = 2$, $\mathbb{K} \neq \mathbb{F}_2$ et $\mathbb{K} \neq \mathbb{F}_3$, on a $D(SL(E)) = D(GL(E)) = SL(E)$.*
5. *Pour $n = 2$, $\mathbb{K} = \mathbb{F}_2$, on a $GL(E) = SL(E)$ et $D(SL(E)) \backsimeq \mathcal{A}_3$.*
6. *Pour $n = 2$ et $\mathbb{K} = \mathbb{F}_3$, on a $D(SL(E)) \backsimeq \mathbb{H}_8$.*

Démonstration.

1. Il est clair que $D(SL(E)) \subset D(GL(E))$.
   Pour tous u, v dans $GL(E)$on a :
   $$\det([u,v]) = \det\left(u \circ v \circ u^{-1} \circ v^{-1}\right) = \det(u)\det(v)\det\left(u^{-1}\right)\det\left(v^{-1}\right) = 1$$
   donc $[u,v] \in SL(E)$.
   On peut aussi utiliser le résultat de l'exercice précédent : $SL(E)$ est un sous groupe distingué de $GL(E)$ et le quotient $\dfrac{GL(E)}{SL(E)} \backsimeq \mathbb{K}^*$ est commutatif, donc $D(GL(E)) \subset SL(E)$.
2. Comme $D(SL(E)) \subset D(GL(E))$, il suffit de montrer que $SL(E) \subset D(SL(E))$.
   Comme $SL(E)$ est engendré par les transvections, il suffit de montrer que toute transvection est dans $D(SL(E))$.
   Si $\tau \neq Id$ est une transvection, il existe alors une base $\mathcal{B}$ de E dans laquelle la matrice de τ est de la forme :
   $$T_n = \begin{pmatrix} I_{n-3} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} I_{n-3} & 0 \\ 0 & T_3 \end{pmatrix}$$

En notant dans $SL_3(\mathbb{K})$:

$$A_3 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ B_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

on a :

$$\begin{aligned} A_3B_3A_3^{-1}B_3^{-1} &= \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= T_3 \end{aligned}$$

En désignant par u, v les automorphismes dans $SL(E)$ de matrices respectives $\begin{pmatrix} I_{n-3} & 0 \\ 0 & A_3 \end{pmatrix}$ et $\begin{pmatrix} I_{n-3} & 0 \\ 0 & B_3 \end{pmatrix}$ dans la base $\mathcal{B}$, on a $\tau = u \circ v \circ u^{-1} \circ v^{-1} \in D(SL(E))$.

3. Pour $n = 2$, la matrice d'une transvection $\tau \neq Id$ est $T_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
   Pour $\lambda \in \mathbb{K}^*$ et $\mu \in \mathbb{K}$, on a dans $GL(E)$:
   $$\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \mu(\lambda - 1) \\ 0 & 1 \end{pmatrix}$$
   Pour $\mathbb{K} \neq \mathbb{F}_2$, prenant $\lambda \in \mathbb{K} \setminus \{0, 1\}$ et $\mu = (\lambda - 1)^{-1}$, on obtient T_2 et $\tau \in D(GL(E))$.
4. Pour $n = 2$, la matrice d'une transvection $\tau \neq Id$ est $T_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
   Pour $\lambda \in \mathbb{K}^*$, on a dans $SL(E)$:
   $$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}^{-1}\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \mu(\lambda^2 - 1) \\ 0 & 1 \end{pmatrix}$$
   Pour $\mathbb{K} \neq \mathbb{F}_2$ et $\mathbb{K} \neq \mathbb{F}_3$ prenant $\lambda \in \mathbb{K} \setminus \{0, 1, -1\}$ et $\mu = (\lambda^2 - 1)^{-1}$, on obtient T_2 et $\tau \in DSL(E)$.
5. Dans $\mathbb{F}_2$, on a $\det(u) = 1$ pour tout $u \in GL(E)$, donc $GL(E) = SL(E)$.
   Voir Perrin ou L2 tout en un, exercices.
6. Voir Perrin ou L2 tout en un, exercices.

■

Exercice 1.15 *En utilisant le fait que le carré d'une transvection est une transvection, montrer que pour $n \geq 3$ et $\mathbb{K}$ de caractéristique différente de 2, on a $D(GL(E)) = D(SL(E)) = SL(E)$.*

Solution 1.15 *Comme dans la démonstration du théorème précédent, il nous suffit de montrer que toute transvection est dans $D(SL(E))$.*
La transvection triviale Id est bien dans $D(SL(E))$.
Pour $n \geq 3$, toutes les transvections différentes de Id sont conjuguées dans $SL(E)$.
Si $\tau_{\varphi,a} \neq Id$ est une transvection, on a alors $\tau_{\varphi,a}^2 = \tau_{\varphi,2a} \neq Id$ en caractéristique différente de 2, donc $\tau_{\varphi,a}$ et $\tau_{\varphi,a}^2$ sont conjuguées dans $SL(E)$, ce qui signifie qu'il existe $u \in SL(E)$ tel que $\tau_{\varphi,a}^2 = u^{-1} \circ \tau_{\varphi,a} \circ u$ et :

$$\tau_{\varphi,a} = u^{-1} \circ \tau_{\varphi,a} \circ u \circ \tau_{\varphi,a}^{-1} = \left[u^{-1}, \tau_{\varphi,a}\right] \in D(SL(E))$$

1.5 Cas des corps finis

On rappelle que si $\mathbb{K}$ est un corps fini à q éléments, on a alors $q = p^r$ où $p \geq 2$ est un nombre premier et r est un entier naturel non nul.

A un isomorphisme près, il n'existe qu'un seul corps fini à $q = p^r$ éléments, c'est $\dfrac{\mathbb{F}_p[X]}{(P)}$ où $P \in \mathbb{F}_p[X]$ est irréductible de degré r.

On note $\mathbb{F}_q$ un tel corps et le nombre premier p est la caractéristique de $\mathbb{F}_q$.

Lemme 1.8 *Pour tout entier p compris entre 1 et n, il y a :*

$$\prod_{k=1}^{p}\left(q^n - q^{k-1}\right) = q^{\frac{p(p-1)}{2}} \prod_{k=n-(p-1)}^{n}\left(q^k - 1\right)$$

familles formées de p vecteurs linéairement indépendants dans E.

Démonstration. Il s'agit de dénombrer l'ensemble des familles $(e_i)_{1\leq i\leq p}$ formées de p vecteurs linéairement indépendants dans E.

Pour choisir e_1 il y a $\operatorname{card}(E\setminus\{0\}) = q^n - 1$ possibilités et pour k compris entre 2 et p, supposant donnés $e_1, \cdots, e_{k-1}$ linéairement indépendants, le vecteur e_k est à choisir dans $E \setminus \bigoplus_{i=1}^{k-1} \mathbb{F}_q e_i$, ce qui laisse $q^n - q^{k-1}$ possibilités.

On a donc un total de :

$$\begin{aligned}\prod_{k=1}^{p}\left(q^n - q^{k-1}\right) &= \prod_{k=1}^{p} q^{k-1}\left(q^{n-(k-1)} - 1\right)\\ &= q^{1+2+\cdots+(p-1)} \prod_{j=n-(p-1)}^{n}\left(q^j - 1\right)\\ &= q^{\frac{p(p-1)}{2}} \prod_{k=n-(p-1)}^{n}\left(q^k - 1\right)\end{aligned}$$

possibilités. ∎

Théorème 1.15 *Pour tout $\mathbb{F}_q$-espace vectoriel E de dimension $n \geq 1$, on a :*

$$\operatorname{card}(GL(E)) = \prod_{k=1}^{n}\left(q^n - q^{k-1}\right) = q^{\frac{n(n-1)}{2}} \prod_{k=1}^{n}\left(q^k - 1\right)$$

et :

$$\operatorname{card}(SL(E)) = q^{n-1}\prod_{k=1}^{n-1}\left(q^n - q^{k-1}\right) = q^{\frac{n(n-1)}{2}} \prod_{k=2}^{n}\left(q^k - 1\right)$$

Démonstration. Comme $GL(E)$ [resp. $SL(E)$] est isomorphe à $GL_n(\mathbb{F}_q)$ [resp. $SL_n(\mathbb{F}_q)$] par le choix d'une base de E, il s'agit de dénombrer $GL_n(\mathbb{F}_q)$ [resp. $SL_n(\mathbb{F}_q)$].

Dire que $A \in GL_n(\mathbb{F}_q)$ revient à dire que ses colonnes forment une base de $\mathbb{F}_q^n$, donc il s'agit de dénombrer toutes les bases $(e_i)_{1\leq i\leq n}$ de $(\mathbb{F}_q)^n$, ce qui nous est donné par le lemme précédent :

$$\operatorname{card}(GL_n(\mathbb{F}_q)) = \prod_{k=1}^{n}\left(q^n - q^{k-1}\right) = q^{\frac{n(n-1)}{2}} \prod_{j=1}^{n}\left(q^j - 1\right)$$

Le groupe quotient $GL_n(\mathbb{F}_q)/SL_n(\mathbb{F}_q)$ étant isomorphe à $\mathbb{F}_q^*$ (théorème 1.3), on a :

$$\begin{aligned}\operatorname{card}(SL_n(\mathbb{F}_q)) &= \frac{\operatorname{card}(GL_n(\mathbb{F}_q))}{\operatorname{card}(\mathbb{F}_q^*)} \\ &= \frac{\prod_{k=1}^{n}(q^n - q^{k-1})}{q-1} = q^{n-1}\prod_{k=1}^{n-1}(q^n - q^{k-1}) \\ &= \frac{q^{\frac{n(n-1)}{2}}\prod_{j=1}^{n}(q^j-1)}{q-1} = q^{\frac{n(n-1)}{2}}\prod_{j=2}^{n}(q^j-1)\end{aligned}$$

■

Corollaire 1.2 *Pour tout entier p compris entre 1 et n, il y a :*

$$\frac{\prod_{k=n-(p-1)}^{n}(q^k-1)}{\prod_{k=1}^{p}(q^k-1)}$$

sous-espaces vectoriels de dimension p dans E.

Démonstration. Notons V_p l'ensemble des familles $(x_i)_{1\leq i\leq p}$ formées de p vecteurs indépendants et W_p l'ensemble de tous les sous-espaces de E de dimension p.

L'application :

$$\begin{array}{rccc}\varphi : & V_p & \to & W_p \\ & (x_i)_{1\leq i\leq p} & \mapsto & \operatorname{Vect}\left((x_i)_{1\leq i\leq p}\right)\end{array}$$

est clairement surjective et les antécédents d'un sous-espace $F \in W_p$ sont toutes les bases de F, donc :

$$\operatorname{card}\left(\varphi^{-1}(F)\right) = \operatorname{card}(GL(F)) = \prod_{k=1}^{p}(q^p - q^{k-1})$$

et en conséquence :

$$\operatorname{card}(V_p) = \operatorname{card}(W_p)\prod_{k=1}^{p}(q^p - q^{k-1})$$

(lemme du berger), ce qui nous donne :

$$\begin{aligned}\operatorname{card}(W_p) &= \frac{\operatorname{card}(V_p)}{\prod_{k=1}^{p}(q^p - q^{k-1})} = \frac{\prod_{k=1}^{p}(q^n - q^{k-1})}{\prod_{k=1}^{p}(q^p - q^{k-1})} \\ &= \frac{q^{\frac{p(p-1)}{2}}\prod_{k=n-(p-1)}^{n}(q^k-1)}{q^{\frac{p(p-1)}{2}}\prod_{k=1}^{p}(q^k-1)} = \frac{\prod_{k=n-(p-1)}^{n}(q^k-1)}{\prod_{k=1}^{p}(q^k-1)}\end{aligned}$$

■

En particulier il a $\dfrac{q^n-1}{q-1}$ droites distinctes et autant d'hyperplans distincts dans E, ce qui peut se voir par dualité (un hyperplan de E est le noyau d'une forme linéaire non nulle définie à une constante multiplicative non nulle près, donc il y a autant d'hyperplans dans E que de droites dans le dual E^*).

En fait cet argument de dualité nous dit que $\operatorname{card}(V_p) = \operatorname{card}(V_{n-p})$ (un sous-espace de dimension p est défini par $n-p$ formes linéaires indépendantes).

Une application originale est donnée par l'exercice suivant d'une grande utilité du point de vue social.

Exercice 1.16 31 *vacanciers se trouvent sur le même bateau durant le mois de Juillet. La capitaine peut inviter chaque soir* 6 *personnes à sa table. Peut-il faire ces invitations chaque soir du mois de Juillet de sorte que chaque vacancier se soit rencontré une fois et une seule ?*

Solution 1.16 *On note E l'espace vectoriel $\mathbb{F}_5^3$. Il y a dans E, $\dfrac{124}{4} = 32$ droites distinctes dans E et autant de plans. Dans chacun de ces plans il y a $\dfrac{5^2-1}{5-1} = \dfrac{24}{4} = 6$ droites distinctes. En identifiant un vacancier à une droite de E, une invitation correspond à un plan de E. En invitant chaque soir du mois de Juillet un plan différent le capitaine est sûr que chaque vacancier s'est rencontré une fois et une seule puisque deux vacanciers distincts (donc deux droites distinctes) définissent un plan.*

Exercice 1.17 *Soient E, F deux $\mathbb{F}_q$-espaces vectoriels de dimensions respectives $n \geq 1$ et $m \geq 1$.*
Montrer que les espaces vectoriels E et F sont isomorphes si, et seulement si, les groupes $GL(E)$ et $GL(F)$ sont isomorphes.

Solution 1.17 *Si les $\mathbb{K}$-espaces vectoriels E, F sont isomorphes ils sont alors de même dimension n (que le corps $\mathbb{K}$ soit fini ou non) et les groupes $GL(E)$, $GL(F)$ sont isomorphes au groupe $GL_n(\mathbb{K})$, donc $GL(E)$ est isomorphe à $GL(F)$.*
Si les groupes $GL(E)$ et $GL(F)$ sont isomorphes, ils sont alors de même cardinal, soit :

$$q^{\frac{n(n-1)}{2}} \prod_{j=1}^{n} \left(q^j - 1\right) = q^{\frac{m(m-1)}{2}} \prod_{j=1}^{m} \left(q^j - 1\right)$$

En supposant que $m > n$, on a :

$$q^{\frac{m(m-1)-n(n-1)}{2}} \prod_{j=n+1}^{m} \left(q^j - 1\right) = 1$$

avec $\displaystyle\prod_{j=n+1}^{m} (q^j - 1) \geq 2$, ce qui est impossible.
On a donc $m = n$ et les espaces vectoriels E et F sont isomorphes.

Le résultat de l'exercice précédent est en fait valable pour un corps commutatif $\mathbb{K}$ quelconque (voir l'exercice 1.1).

Exercice 1.18 *Soient $\mathbb{L}$ un corps commutatif et m un entier naturel non nul. Montrer que si les groupes $GL_n(\mathbb{F}_q)$ et $GL_m(\mathbb{L})$ sont isomorphes, $\mathbb{L}$ est alors isomorphe à $\mathbb{F}_q$ et $n = m$.*

Solution 1.18 *Si $GL_m(\mathbb{L})$ est isomorphe à $GL_n(\mathbb{F}_q)$ il en est alors de même de leurs centres respectifs $\mathbb{L}^* I_m$ et $\mathbb{F}_q^* I_n$, donc* $\operatorname{card}(\mathbb{L}^*) = q-1$ *et $\mathbb{L}$ est un corps à q éléments, donc isomorphe à $\mathbb{F}_q$. L'exercice précédent nous dit alors que $n = m$.*

Exercice 1.19 *On note :*

$$\mu_n(\mathbb{F}_q) = \{z \in \mathbb{F}_q \mid z^n = 1\}$$

l'ensemble des racines n-èmes de l'unité dans $\mathbb{F}_q$.
C'est un sous-groupe cyclique du groupe multiplicatif $\left(\mathbb{F}_q^*, \cdot\right)$ (lemme 1.1).

1. *En désignant par δ le* pgcd *de n et $q-1$, montrer que $\mu_n(\mathbb{F}_q) = \mu_\delta(\mathbb{F}_q)$.*
2. *Montrer que :*
$$\operatorname{card}(\mu_n(\mathbb{F}_q)) = n \wedge (q-1)$$
3. *On note $Z(G)$ le centre d'un groupe G et E est un $\mathbb{F}_q$-espace vectoriel de dimension $n \geq 1$. Montrer que l'on a :*
$$\operatorname{card}(Z(GL(E))) = q-1$$
et :
$$\operatorname{card}(Z(SL(E))) = n \wedge (q-1)$$

Solution 1.19

1. *Comme $\delta = n \wedge (p-1)$ divise n, l'équation $z^\delta = 1$ entraîne $z^n = 1$, donc $\mu_\delta(\mathbb{F}_q) \subset \mu_n(\mathbb{F}_q)$. Si $z \in \mu_n(\mathbb{F}_q)$, on a alors $z^n = 1$ et l'ordre m de z dans le groupe multiplicatif $\mathbb{F}_q^*$ divise n.*
Le théorème de Lagrange nous dit que m divise aussi $q-1 = \operatorname{card}\left(\mathbb{F}_q^*\right)$, donc m qui est un diviseur commun de n et $q-1$ est aussi un diviseur du pgcd *δ, ce qui entraîne que $z^\delta = 1$, soit que $z \in \mu_\delta(\mathbb{F}_q)$.*
On a donc $\mu_\delta(\mathbb{F}_q) \subset \mu_n(\mathbb{F}_q)$ et l'égalité $\mu_n(\mathbb{F}_q) = \mu_\delta(\mathbb{F}_q)$.
2. *Comme δ divise $q-1$, le polynôme $X^\delta - 1$ divise $X^{q-1} - 1 = \prod_{\lambda \in \mathbb{F}_q^*} (X - \lambda)$ (encore le théorème de Lagrange), ce qui implique que l'équation $X^\delta - 1 = 0$ a δ racines dans $\mathbb{F}_q^*$.*
On a donc :
$$\operatorname{card}(\mu_n(\mathbb{F}_q)) = \operatorname{card}(\mu_\delta(\mathbb{F}_q)) = \delta = n \wedge (q-1)$$
En particulier, pour n premier avec $q-1$, on a $\mu_n(\mathbb{F}_q) = \{1\}$.
3. *On a :*
$$\operatorname{card}(Z(GL(E))) = \operatorname{card}\left(\mathbb{F}_q^* \cdot I_d\right) = q-1$$
et :
$$\operatorname{card}(Z(SL(E))) = \operatorname{card}(\mu_n(\mathbb{F}_q) \cdot I_d) = n \wedge (q-1)$$
En particulier, pour n premier avec $q-1$, on a $Z(SL(E)) = \{I_n\}$.

Le théorème 1.15 peut être utilisé pour démontrer le premier théorème de Sylow qui nous dit que si G est un groupe fini d'ordre $n = p^\alpha m$ où $p \geq 2$ est un nombre premier ne divisant pas $m \geq 1$ et α un entier naturel non nul, il existe alors un sous-groupe H de G d'ordre p^α (on dit que H est un p-sous-groupe de Sylow de G).

La connaissance d'un p-sous-groupe de Sylow de $GL_n(\mathbb{F}_p)$ pour tout nombre premier $p \geq 2$ et tout entier $n \geq 2$ permet de prouver l'existence d'un p-sous-groupe de Sylow de tout groupe G de cardinal $n = p^\alpha m$ où m est premier avec p.

En écrivant que :

$$\operatorname{card}\left(GL_n\left(\mathbb{F}_p\right)\right) = p^{\frac{n(n-1)}{2}} \prod_{j=1}^{n} \left(p^j - 1\right) = p^\alpha m$$

l'entier $m = \prod_{j=1}^{n} \left(p^j - 1\right)$ étant premier avec p et $\alpha = \frac{n(n-1)}{2} \geq 1$ pour $n \geq 2$, on vérifie facilement que le sous ensemble $T_n\left(\mathbb{F}_p\right)$ de $GL_n\left(\mathbb{F}_p\right)$ formé des matrices triangulaires supérieures de termes diagonaux tous égaux à 1 est un sous-groupe de $GL_n\left(\mathbb{F}_p\right)$.

En effet, pour toute matrice $A \in T_n\left(\mathbb{F}_p\right)$, on a $\det\left(A\right) = 1$, donc $T_n\left(\mathbb{F}_p\right) \subset GL_n\left(\mathbb{F}_p\right)$.

La matrice I_n est dans $T_n\left(\mathbb{F}_p\right)$, le produit de deux matrices de $T_n\left(\mathbb{F}_p\right)$ et l'inverse d'une matrice de $T_n\left(\mathbb{F}_p\right)$ sont dans $T_n\left(\mathbb{F}_p\right)$, donc $T_n\left(\mathbb{F}_p\right)$ est bien un sous-groupe de $GL_n\left(\mathbb{F}_p\right)$.

L'application qui associe à une matrice $A = \left(\left(a_{i,j}\right)\right)_{1 \leq i,j \leq n} \in T_n\left(\mathbb{F}_p\right)$ l'élément $\left(a_{i,j}\right)_{1 \leq i < j \leq n} \in \mathbb{F}_p^{\frac{n(n-1)}{2}}$ étant bijective, on a :

$$\operatorname{card}\left(T_n\left(\mathbb{F}_p\right)\right) = \operatorname{card}\left(\mathbb{F}_p^{\frac{n(n-1)}{2}}\right) = p^{\frac{n(n-1)}{2}}$$

Ce groupe $T_n\left(\mathbb{F}_p\right)$ est donc un p-Sylow de $GL_n\left(\mathbb{F}_p\right)$ (et aussi de $SL_n\left(\mathbb{F}_p\right)$).

On peut remarquer que le polynôme caractéristique d'une matrice $A \in T_n\left(\mathbb{F}_p\right)$ est $\left(X-1\right)^n$.

Comme tous les p-Sylow de $GL_n\left(\mathbb{F}_p\right)$ sont conjugués (deuxième théorème de Sylow), on en déduit que les p-Sylow de $GL_n\left(\mathbb{F}_p\right)$ sont les $G = P^{-1} T_n\left(\mathbb{F}_p\right) P$, où $P \in GL_n\left(\mathbb{F}_p\right)$. Toutes les matrices d'un tel groupe G ont $\left(X-1\right)^n$ pour polynôme caractéristique et sont unipotentes (i. e. $\left(A - I_n\right)^n = 0$).

En utilisant un théorème de Cayley et les matrices de permutations, on peut montrer que tout groupe fini d'ordre $n \geq 1$ est isomorphe à un sous-groupe de $GL_n\left(\mathbb{F}_p\right)$, quel que soit le nombre premier p (corollaire **??**).

Ce résultat permet de montrer le premier théorème de Sylow.

Théorème 1.16 *Si G est un groupe d'ordre $p^\alpha m$ avec $\alpha \geq 1$ et p premier ne divisant pas m, il existe alors un p-sous-groupe de Sylow de G.*

Démonstration. On dispose de $H = T_n\left(\mathbb{F}_p\right)$ qui est un p-Sylow de $GL_n\left(\mathbb{F}_p\right)$ et G est identifié à un sous-groupe de $GL_n\left(\mathbb{F}_p\right)$.

On fait agir le groupe G sur l'ensemble $E = GL_n\left(\mathbb{F}_p\right)/H$ des classes à gauche modulo H par :

$$\left(g, \overline{A}\right) = \left(g, A \cdot H\right) \mapsto \overline{gA} = \left(gA\right) \cdot H$$

Comme :

$$\operatorname{Card}\left(E\right) = \frac{\operatorname{Card}\left(GL_n\left(\mathbb{F}_p\right)\right)}{\operatorname{Card}\left(H\right)} = \frac{p^{\frac{n(n-1)}{2}} q}{p^{\frac{n(n-1)}{2}}} = q$$

est premier avec p et les orbites de l'action considérée forment une partition de E, il existe un élément $\overline{A}$ de E dont l'orbite est de cardinal r premier avec p.

On vérifie alors que le stabilisateur de $\overline{A}$ est un p-Sylow de G.

Ce stabilisateur est :

$$\begin{aligned} K = \operatorname{Stab}\left(\overline{A}\right) &= \left\{g \in G \mid g \cdot \overline{A} = \overline{A}\right\} = \left\{g \in G \mid \left(gA\right) \cdot H = A \cdot H\right\} \\ &= \left\{g \in G \mid \left(A^{-1} g A\right) \cdot H = H\right\} \\ &= \left\{g \in G \mid \left(A^{-1} g A\right) \in H\right\} = G \cap \left(AHA^{-1}\right) \end{aligned}$$

donc $\mathrm{Card}\,(K)$ divise $\mathrm{Card}\,(AHA^{-1}) = \mathrm{Card}\,(H) = p^{\frac{n(n-1)}{2}}$, c'est-à-dire que $\mathrm{Card}\,(K) = p^{\beta}$ avec β compris entre 0 et $\dfrac{n\,(n-1)}{2}$.

Comme $G/\,\mathrm{Stab}\left(\overline{A}\right)$ est de même cardinal que l'orbite $G\cdot\overline{A}$, on a :

$$r = \mathrm{Card}\left(G/\,\mathrm{Stab}\left(\overline{A}\right)\right) = \frac{\mathrm{Card}\,(G)}{\mathrm{Card}\,(K)} = \frac{p^{\alpha}m}{p^{\beta}} = p^{\alpha-\beta}m$$

qui est premier avec p ($p^{\alpha-\beta}m$ est entier avec p premier qui ne divise pas m, donc $\alpha-\beta\geq 0$), ce qui impose $\beta=\alpha$ et K est un p-Sylow de G. ∎

Le théorème 1.15 peut être utilisé pour dénombrer l'ensemble $\mathcal{N}_n\,(\mathbb{F}_q)$ des matrices $A\in\mathcal{M}_n\,(\mathbb{F}_q)$ qui sont nilpotentes d'ordre $n\geq 2$ (l'ordre maximal).

Pour ce faire, on note :

$$J = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 1 & 0 \end{pmatrix}$$

et on fait agir le groupe $GL_n\,(\mathbb{F}_q)$ sur l'ensemble $\mathcal{M}_n\,(\mathbb{F}_q)$ par conjugaison :

$$(P,A)\in GL_n\,(\mathbb{F}_q)\times\mathcal{M}_n\,(\mathbb{F}_q)\mapsto PAP^{-1}\in\mathcal{M}_n\,(\mathbb{F}_q)$$

Lemme 1.9 *La matrice J est nilpotente d'ordre n.*

Démonstration. Le polynôme caractéristique de J est $\chi_J\,(X)=X^n$, donc $J^n=0$.

En désignant par $(e_k)_{1\leq k\leq n}$ la base canonique de $\mathbb{F}_q^n$, on a :

$$\begin{cases} Je_k = e_{k+1} \ (1\leq k\leq n-1) \\ Je_n = 0 \end{cases}$$

donc :

$$J^{k-1}e_1 = e_k \ (1\leq k\leq n)$$

et en particulier $J^{n-1}e_1=e_n\neq 0$ et $J^{n-1}\neq 0$.

Donc J est nilpotente d'ordre n. ∎

Lemme 1.10 *L'ensemble $\mathcal{N}_n\,(\mathbb{F}_q)$ est l'orbite de J sous l'action de $GL_n\,(\mathbb{F}_q)$ par conjugaison.*

Démonstration. C'est simplement le fait que toute matrice nilpotente d'ordre n est semblable à J (réduction de Jordan).

L'orbite de J sous l'action de $GL_n\,(\mathbb{F}_q)$ est l'ensemble :

$$\mathcal{O}\,(J) = \left\{PJP^{-1} \mid P\in GL_n\,(\mathbb{F}_q)\right\}$$

de toutes les matrices semblables à J.

Pour toute matrice $P\in GL_n\,(\mathbb{F}_q)$ et tout entier naturel k, on a $\left(PJP^{-1}\right)^k = PJ^kP^{-1}$, donc PJP^{-1} est nilpotente d'ordre n.

On a donc l'inclusion $\mathcal{O}\,(J)\subset\mathcal{N}_n\,(\mathbb{F}_q)$.

L'endomorphisme $u\in\mathcal{L}\left(\mathbb{F}_q^n\right)$ de matrice $A\in\mathcal{N}_n\,(\mathbb{F}_q)$ dans la base canonique $(e_k)_{1\leq k\leq n}$ de $\mathbb{F}_q^n$ est aussi nilpotent d'ordre n, donc il existe un vecteur $x\in\mathbb{F}_q^n\setminus\{0\}$ tel que $u^{n-1}\,(x)\neq 0$.

On vérifie alors que la famille $\left(u^k(x)\right)_{0\leq k\leq n-1}$ est une base $\mathbb{F}_q^n$. En effet, si il existe $(a_k)_{0\leq k\leq n-1} \in \mathbb{F}_q^n \setminus \{0\}$ tel que $\sum_{k=0}^{n-1} a_k u^k(x) = 0$, en désignant par p le plus petit indice compris entre 0 et $n-1$ tel que $a_p \neq 0$, on a :

$$0 = u^{n-1-p}\left(\sum_{k=0}^{n-1} a_k u^k(x)\right) = u^{n-1-p}\left(\sum_{k=p}^{n-1} a_k u^k(x)\right) = a_p u^{n-1}(x)$$

ce qui n'est pas possible. Cette famille est donc libre et c'est une base car formée de n éléments.

La matrice de u dans cette nouvelle base est alors la matrice J qui est donc semblable à J et en conséquence dans $\mathcal{O}(J)$. ■

On a donc :

$$\operatorname{card}(\mathcal{N}_n(\mathbb{F}_q)) = \operatorname{card}(\mathcal{O}(J)) = \frac{\operatorname{card}(GL_n(\mathbb{F}_q))}{\operatorname{card}(Stab(J))}$$

et il s'agit de déterminer le stabilisateur de J sous l'action de $GL_n(\mathbb{F}_q)$.

Lemme 1.11 *Le stabilisateur de J sous l'action de $GL_n(\mathbb{F}_q)$ est :*

$$Stab(J) = GL_n(\mathbb{F}_q) \cap \mathbb{F}_q[J]$$

où $\mathbb{F}_q[J]$ est l'ensemble des polynômes en J.

Démonstration. Le stabilisateur de J sous l'action de $GL_n(\mathbb{F}_q)$ est le commutant de J :

$$\begin{aligned} Stab(J) &= \left\{P \in GL_n(\mathbb{F}_q) \mid PJP^{-1} = J\right\} \\ &= \{P \in GL_n(\mathbb{F}_q) \mid PJ = JP\} \end{aligned}$$

et il est clair que $GL_n(\mathbb{F}_q) \cap \mathbb{F}_q[J] \subset Stab(J)$.

En désignant par $(e_k)_{1\leq k\leq n}$ la base canonique de $\mathbb{F}_q^n$, on a pour toute matrice $A \in Stab(J)$:

$$Ae_1 = \sum_{k=1}^{n} a_{k,1} e_k = \sum_{k=1}^{n} a_{k,1} J^{k-1} e_1 = R(J)\, e_1$$

où $R = \sum_{k=1}^{n-1} a_{k,1} X^{k-1} \in \mathbb{F}_q[X]$ et pour p compris entre 2 et n :

$$\begin{aligned} R(J)\, e_p &= R(J)\left(J^{p-1} e_1\right) = J^{p-1}\left(R(J)\, e_1\right) \\ &= J^{p-1}(Ae_1) = A\left(J^{p-1} e_1\right) = Ae_p \end{aligned}$$

(A commute à J).

On a donc $A = R(J) \in GL_n(\mathbb{F}_q) \cap \mathbb{F}_q[J]$.

D'où l'égalité $Stab(J) = GL_n(\mathbb{F}_q) \cap \mathbb{F}_q[J]$. ■

Théorème 1.17 *On a :*

$$\operatorname{card}(\mathcal{N}_n(\mathbb{F}_q)) = \prod_{k=1}^{n-1}\left(q^n - q^{k-1}\right)$$

Démonstration. Par division euclidienne, on a :

$$\mathbb{F}_q[J] = \{R(J) \mid R \in \mathbb{F}_q[X] \text{ et } \deg(R) \leq n-1\}$$

(X^n est le polynôme minimal de J).

Pour $R = \sum_{k=0}^{n-1} a_k X^k \in \mathbb{F}_q[X]$, on a :

$$R(J) = \begin{pmatrix} a_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ a_{n-1} & \cdots & a_1 & a_0 \end{pmatrix}$$

donc $R \in GL_n(\mathbb{F}_q)$ si, et seulement si, $a_0 \neq 0$ et comme un élément de $\mathbb{F}_q[J]$ s'écrit de manière unique $\sum_{k=0}^{n-1} a_k J^k$, on en déduit que :

$$\begin{aligned} \operatorname{card}(Stab(J)) &= \operatorname{card}\left\{\sum_{k=0}^{n-1} a_k X^k \mid (a_k)_{0\leq k\leq n-1} \in \mathbb{F}_q^* \times \mathbb{F}_q^{n-1}\right\} \\ &= (q-1)\, q^{n-1} \end{aligned}$$

et :

$$\begin{aligned} \operatorname{card}(\mathcal{N}_n(\mathbb{F}_q)) = \operatorname{card}(\mathcal{O}(J)) &= \frac{\operatorname{card}(GL_n(\mathbb{F}_q))}{\operatorname{card}(Stab(J))} \\ &= \frac{\prod_{k=1}^{n}\left(q^n - q^{k-1}\right)}{(q-1)\, q^{n-1}} = \prod_{k=1}^{n-1}\left(q^n - q^{k-1}\right) \end{aligned}$$

■

On peut montrer, mais c'est plus difficile que le nombre de matrices nilpotentes de $\mathcal{M}_n(\mathbb{F}_q)$ est q^{n^2-n} (Tosel, RMS 177-1, 2006/2007).

Le théorème 1.15 peut aussi être utilisé pour dénombrer les automorphismes diagonalisables d'un $\mathbb{F}_q$-espace vectoriel de dimension $n \geq 1$.

Pour ce qui suit E un $\mathbb{F}_q$-espace vectoriel de dimension $n \geq 1$ et on désigne par $DL(E)$ l'ensemble des automorphismes de E qui sont diagonalisables.

Lemme 1.12 *On a :*

$$DL(E) = \left\{u \in GL(E) \mid u^{q-1} = Id\right\}$$

Démonstration. Il s'agit de montrer que $u \in GL(E)$ est diagonalisable si, et seulement si, on a $u^{q-1} = Id$.

Si $u \in GL(E)$ est diagonalisable, son polynôme minimal est alors scindé à racines simples, soit $\pi_u(X) = \prod_{\lambda \in \mathrm{Sp}(u)} (X - \lambda)$ avec $\mathrm{Sp}(u) \subset \mathbb{F}_q^*$ et comme π_u divise $X^{q-1} - 1 = \prod_{\lambda \in \mathbb{F}_q^*} (X - \lambda)$, on a $u^{q-1} = Id$.

Réciproquement, si $u \in GL(E)$ est tel que $u^{q-1} = Id$, le polynôme $X^{q-1} - 1$ qui est scindé à racines simples dans $\mathbb{F}_q[X]$ (on a $X^{q-1} - 1 = \prod_{\lambda \in \mathbb{F}_p^*} (X - \lambda)$ d'après le théorème de Lagrange) annule u, donc u est diagonalisable. ■

De manière analogue, on voit que $u \in \mathcal{L}(E)$ est diagonalisable si, et seulement si, $u^q = u$.

On note $\mathbb{F}_q^* = \{\lambda_1, \cdots, \lambda_{q-1}\}$.

Lemme 1.13 *Pour tout $u \in DL(E)$, on a :*

$$E = \bigoplus_{k=1}^{q-1} \ker(u - \lambda_k Id)$$

Démonstration. Tout automorphisme $u \in DL(E)$ étant annulé par le polynôme $P(X) = X^{q-1} - 1 = \prod_{k=1}^{q-1} (X - \lambda_k)$ le théorème de décomposition des noyaux nous dit que :

$$E = \bigoplus_{k=1}^{q-1} \ker(u - \lambda_k Id)$$

■

On désigne par $\mathcal{F}$ l'ensemble des suites $(E_k)_{1 \leq k \leq q-1}$ de sous-espaces vectoriels de E tels que $E = \bigoplus_{k=1}^{q-1} E_k$.

Lemme 1.14 *L'application :*

$$\begin{array}{rccc} \varphi : & DL(E) & \to & \mathcal{F} \\ & u & \mapsto & (\ker(u - \lambda_k Id))_{1 \leq k \leq q-1} \end{array}$$

est bijective.

Démonstration. Le lemme précédent nous dit que l'application φ est bien à valeurs dans $\mathcal{F}$.

Pour u, v dans $DL(E)$ tels que $\varphi(u) = \varphi(v)$, on a $\ker(u - \lambda_k Id) = \ker(v - \lambda_k Id)$ pour tout k compris entre 1 et $q-1$, donc $u(x) = v(x) = \lambda_k x$ pour tout $x \in \ker(u - \lambda_k Id)$ et tout k compris entre 1 et $q-1$, ce qui entraîne que $u = v$ puisque $E = \bigoplus_{k=1}^{q-1} \ker(u - \lambda_k Id)$, donc φ est injective.

Pour $(E_k)_{1 \leq k \leq q-1} \in \mathcal{F}$, l'application linéaire u définie par $u_{|E_k} = \lambda_k Id_{E_k}$ pour tout k compris entre 1 et $q-1$ est dans $DL(E)$ telle que $\varphi(u) = (E_1, \cdots, E_{q-1})$, donc φ est surjective. ■

On a donc :

$$\operatorname{card}(DL(E)) = \operatorname{card}(\mathcal{F})$$

et il s'agit alors de dénombrer $\mathcal{F}$.

Pour $(n_k)_{1 \leq k \leq q-1} \in \mathbb{N}^{q-1}$ tel que $\sum_{k=1}^{q-1} n_k = n$, on note :

$$\mathcal{F}_{(n_1, \cdots, n_{q-1})} = \left\{ (E_k)_{1 \leq k \leq q-1} \in \mathcal{F} \mid \dim(E_k) = n_k,\ 1 \leq k \leq q-1 \right\}$$

ce qui nous donne une partition de $\mathcal{F}$ et il s'agit de dénombrer chaque $\mathcal{F}_{(n_1, \cdots, n_{q-1})}$.

Lemme 1.15 *Pour $(n_k)_{1\leq k\leq q-1}\in\mathbb{N}^{q-1}$ fixé tel que $\sum_{k=1}^{q-1}n_k=n$, l'application :*

$$\begin{array}{ccc} GL(E)\times\mathcal{F}_{(n_1,\cdots,n_{q-1})} & \to & \mathcal{F}_{(n_1,\cdots,n_{q-1})} \\ (u,(E_1,\cdots,E_{q-1})) & \mapsto & u\cdot(E_1,\cdots,E_{q-1})=(u(E_1),\cdots,u(E_{q-1})) \end{array}$$

définit une action transitive (i. e. à une seule orbite) de $GL(E)$ sur $\mathcal{F}_{(n_1,\cdots,n_{q-1})}$.

Démonstration. Pour $u\in GL(E)$ et $E=\bigoplus_{k=1}^{q-1}E_k$ avec $\dim(E_k)=n_k$ pour tout k compris entre 1 et $n-1$, on a $E=u(E)=\sum_{k=1}^{q-1}u(E_k)$ avec $\dim(u(E_k))=\dim(E_k)=n_k$, donc $E=\bigoplus_{k=1}^{q-1}u(E_k)$, c'est-à-dire que $(u(E_k))_{1\leq k\leq q-1}\in\mathcal{F}_{(n_1,\cdots,n_{q-1})}$.

Il est facile de vérifier que l'on définit bien une action de groupe.

Montrer que cette action est transitive revient à montrer que pour tout $(E_k)_{1\leq k\leq q-1}$ dans $\mathcal{F}_{(n_1,\cdots,n_{q-1})}$, on a :

$$GL(E)\cdot(E_1,\cdots,E_{q-1})=\mathcal{F}_{(n_1,\cdots,n_{q-1})}$$

c'est-à-dire que pour tout $(F_k)_{1\leq k\leq q-1}$ dans $\mathcal{F}_{(n_1,\cdots,n_{q-1})}$, il existe $u\in GL(E)$ telle que $u(E_k)=F_k$ pour tout k compris entre 1 et $q-1$.

Pour ce faire on se donne deux bases $\mathcal{B}=\bigcup_{\substack{k=1\\n_k\geq 1}}^{q-1}\mathcal{B}_k$ et $\mathcal{B}'=\bigcup_{\substack{k=1\\n_k\geq 1}}^{q-1}\mathcal{B}'_k$ de E telles que pour tout k compris entre 1 et $q-1$, $\mathcal{B}_k$ est une base de E_k et $\mathcal{B}'_k$ une base de F_k.

Comme $\dim(E_k)=\dim(F_k)=n_k$, on peut définir $u\in GL(E)$ par $u(\mathcal{B}_k)=\mathcal{B}'_k$ pour tout k compris entre 1 et $q-1$ et cet automorphisme est tel que $u(E_k)=F_k$ pour tout k compris entre 1 et $q-1$. ∎

Lemme 1.16 *En notant, pour $(n_k)_{1\leq k\leq q-1}\in\mathbb{N}^{q-1}$ tel que $\sum_{k=1}^{q-1}n_k=n$ et $(E_k)_{1\leq k\leq q-1}$ fixé dans $\mathcal{F}_{(n_1,\cdots,n_{q-1})}$:*

$$\mathrm{Stab}(E_1,\cdots,E_{q-1})=\{u\in GL(E)\mid u(E_k)=E_k,\ 1\leq k\leq q-1\}$$

le stabilisateur de $(E_k)_{1\leq k\leq q-1}$, on a :

$$\mathrm{card}(\mathrm{Stab}(E_1,\cdots,E_{q-1}))=\prod_{k=1}^{q-1}\mathrm{card}(GL(E_k))$$

et :

$$\mathrm{card}\left(\mathcal{F}_{(n_1,\cdots,n_{q-1})}\right)=\frac{\mathrm{card}(GL(E))}{\prod_{k=1}^{q-1}\mathrm{card}(GL(E_k))}$$

Démonstration. Pour tout $u\in\mathrm{Stab}(E_1,\cdots,E_{q-1})$ et tout k compris entre 1 et $q-1$, on a $u(E_k)=E_k$, donc $u_{|E_k}\in GL(E_k)$.

Réciproquement si $u\in GL(E)$ est tel que $u_{|E_k}\in GL(E_k)$ pour tout k compris entre 1 et $q-1$, on a alors $u(E_k)=E_k$.

On a donc :

$$\mathrm{Stab}\left(E_1,\cdots,E_{q-1}\right)=\left\{u\in GL\left(E\right)\mid u_{|E_k}\in GL\left(E_k\right)\ 1\leq k\leq q-1\right\}$$

et en conséquence :

$$\mathrm{card}\left(\mathrm{Stab}\left(E_1,\cdots,E_{q-1}\right)\right)=\prod_{k=1}^{q-1}\mathrm{card}\left(GL\left(E_k\right)\right)$$

Comme il y a une seule orbite, on a :

$$\begin{aligned}\mathrm{card}\left(\mathcal{F}_{(n_1,\cdots,n_{q-1})}\right)&=\mathrm{card}\left(GL\left(E\right)\cdot\left(E_1,\cdots,E_{q-1}\right)\right)=\frac{\mathrm{card}\left(GL\left(E\right)\right)}{\mathrm{card}\left(\mathrm{Stab}\left(E_1,\cdots,E_{q-1}\right)\right)}\\&=\frac{\mathrm{card}\left(GL\left(E\right)\right)}{\prod\limits_{k=1}^{q-1}\mathrm{card}\left(GL\left(E_k\right)\right)}\end{aligned}$$

■

Théorème 1.18 *On a :*

$$\mathrm{card}\left(DL\left(E\right)\right)=\sum_{\substack{(n_1,\cdots,n_{q-1})\in\mathbb{N}^{q-1}\\ n_1+\cdots+n_{q-1}=n}}\frac{\mathrm{card}\left(GL_n\left(\mathbb{F}_q\right)\right)}{\mathrm{card}\left(GL_{n_1}\left(\mathbb{F}_q\right)\right)\cdots\mathrm{card}\left(GL_{n_{q-1}}\left(\mathbb{F}_q\right)\right)}$$

avec la convention $\mathrm{card}\left(GL_0\left(\mathbb{F}_q\right)\right)=1$.

Démonstration. Les $\mathcal{F}_{(n_1,\cdots,n_{q-1})}$ formant une partition de $\mathcal{F}$, on aboutit à :

$$\begin{aligned}\mathrm{card}\left(DL\left(E\right)\right)=\mathrm{card}\left(\mathcal{F}\right)&=\sum_{\substack{(n_1,\cdots,n_{q-1})\in\mathbb{N}^{q-1}\\ n_1+\cdots+n_{q-1}=n}}\mathrm{card}\left(\mathcal{F}_{(n_1,\cdots,n_{q-1})}\right)\\&=\sum_{\substack{(n_1,\cdots,n_{q-1})\in\mathbb{N}^{q-1}\\ n_1+\cdots+n_{q-1}=n}}\frac{\mathrm{card}\left(GL\left(E\right)\right)}{\prod\limits_{k=1}^{q-1}\mathrm{card}\left(GL\left(E_k\right)\right)}\end{aligned}$$

■

Exercice 1.20 *On se donne un morphisme de groupes* γ *de* $GL_n\left(\mathbb{F}_q\right)$ *dans* $\mathbb{F}_q^*$.

1. *Montrer qu'il existe un entier naturel* r *compris entre* 0 *et* $q-2$ *tel que pour toute matrice de la dilatation* $D_n\left(\lambda\right)=\begin{pmatrix}I_{n-1}&0\\0&\lambda\end{pmatrix}$ *avec* $\lambda\in\mathbb{F}_q^*$, *on a* $\gamma\left(D_n\left(\lambda\right)\right)=\lambda^r$.
2. *Montrer que, pour toute matrice de transvection* $T_{ij}\left(\lambda\right)=I_n+\lambda E_{ij}$ *où* $1\leq i\neq j\leq n$ *et* $\lambda\in\mathbb{F}_q$, *on a* $\gamma\left(T_{ij}\left(\lambda\right)\right)=1$.
3. *Déduire de ce qui précède que :*

$$\forall A\in GL_n\left(\mathbb{F}_q\right),\ \gamma\left(A\right)=\left(\det\left(A\right)\right)^r$$

Solution 1.20

1. *Soit* $D_n(\lambda)=\begin{pmatrix} I_{n-1} & 0 \\ 0 & \lambda \end{pmatrix}$ *une matrice de la dilatation avec* $\lambda\in\mathbb{K}\setminus\{0,1\}$.
   Comme $\mathbb{F}_q$ *est un corps fini, le groupe multiplicatif* $\mathbb{F}_q^*$ *est cyclique, il existe donc* $\mu\in\mathbb{F}_q^*$ *tel que* $\mathbb{F}_q^*=\langle\mu\rangle=\{1,\mu,\cdots,\mu^{q-2}\}$.
   On a donc $\lambda=\mu^k$ *où* k *est un entier compris entre* 0 *et* $q-2$ *et :*
   $$D_n(\lambda)=\begin{pmatrix} I_{n-1} & 0 \\ 0 & \lambda \end{pmatrix}=(D_n(\mu))^k$$
   Il en résulte que $\gamma(D_n(\lambda))=\gamma(D_n(\mu))^k$.
   Puis en écrivant que $\gamma(D_n(\mu))=\mu^r$ *dans* $\mathbb{F}_q^*$, *où* r *est un entier compris entre* 0 *et* $q-2$ *(indépendant de la matrice de dilatation* $D_n(\lambda)$*), on déduit que* $\gamma(D_n(\lambda))=\mu^{rk}=\left(\mu^k\right)^r=\lambda^r$.
2. *Pour* $1\leq i\neq j\leq n$ *fixés, l'application :*
   $$\varphi:\lambda\in\mathbb{F}_q\mapsto\gamma(T_{ij}(\lambda))\in\mathbb{F}_q^*$$
   est un morphisme de groupes de $(\mathbb{F}_q,+)$ *dans* $\left(\mathbb{F}_q^*,\cdot\right)$.
   En effet, pour λ,μ *dans* $\mathbb{F}_q$, *on a* $\varphi(\lambda+\mu)=\gamma(T_{ij}(\lambda+\mu))$ *avec :*
   $$\begin{aligned} T_{ij}(\lambda+\mu)&=I_n+(\lambda+\mu)E_{ij}=(I_n+\lambda E_{ij})(I_n+\mu E_{ij})\\ &=T_{ij}(\lambda)T_{ij}(\mu)\end{aligned}$$
   puisque $E_{ij}^2=0$ *pour* $i\neq j$, *donc :*
   $$\begin{aligned}\varphi(\lambda+\mu)&=\gamma(T_{ij}(\lambda)T_{ij}(\mu))=\gamma(T_{ij}(\lambda))\gamma(T_{ij}(\mu))\\ &=\varphi(\lambda)\varphi(\mu)\end{aligned}$$
   Ces groupes étant finis, on a :
   $$\operatorname{card}(\mathbb{F}_q)=\operatorname{card}(\ker(\varphi))\operatorname{card}(\operatorname{Im}(\varphi))$$
   c'est-à-dire que $\operatorname{card}(\operatorname{Im}(\varphi))$ *divise* $q=\operatorname{card}(\mathbb{F}_q)$.
   Mais $\operatorname{Im}(\varphi)$ *étant un sous-groupe de* $\mathbb{F}_q^*$ *a un cardinal qui divise* $q-1$ *et nécessairement* $\operatorname{card}(\operatorname{Im}(\varphi))=1$ *du fait que* q *et* $q-1$ *sont premiers entre eux.*
   On a donc $\operatorname{Im}(\varphi)=\{\varphi(0)\}=\{1\}$, *ce qui signifie que* φ *est la fonction constante égale à* 1 *ou encore que* $\gamma(T_{ij}(\lambda))=1$ *pour tout* $\lambda\in\mathbb{F}_q$.
3. *Résulte du fait que toute matrice* $A\in GL_n(\mathbb{F}_q)$ *est produit de matrices de transvections (si elle est dans* $SL_n(\mathbb{F}_q)$*) ou d'une matrice de dilatation de rapport* $\det(A)$ *et de matrices de transvections (si elle n'est pas dans* $SL_n(\mathbb{F}_q)$*).*

1.6 Topologie sur $GL(E)$ ($\mathbb{K}=\mathbb{R}$ ou $\mathbb{K}=\mathbb{C}$)

On suppose ici que $\mathbb{K}=\mathbb{R}$ ou $\mathbb{K}=\mathbb{C}$, $(E,\|\cdot\|)$ est un $\mathbb{K}$-espace vectoriel normé de dimension finie $n\geq 1$ et l'espace vectoriel $\mathcal{L}(E)$ est muni de la norme induite définie par :

$$\forall u\in\mathcal{L}(E),\ \|u\|=\sup_{\|x\|=1}\|u(x)\|=\sup_{x\in E\setminus\{0\}}\frac{\|u(x)\|}{\|x\|}$$

Comme $\mathcal{L}(E)$ est de dimension finie, toutes les normes sur cet espace sont équivalentes et tout endomorphisme de $\mathcal{L}(E)$ est continue.

Dans le cas où $(E, \langle \cdot \mid \cdot \rangle)$ est un espace réel euclidien de dimension $n \geq 1$, on rappelle qu'un endomorphisme $u \in \mathcal{L}(E)$ est dit orthogonal (ou que c'est une isométrie) si :

$$\forall (x, y) \in E^2,\ \langle u(x) \mid u(y) \rangle = \langle x \mid y \rangle$$

ce qui est encore équivalent à :

$$\forall x \in E,\ \|u(x)\| = \|x\|$$

On note $\mathcal{O}(E)$ l'ensemble des endomorphismes orthogonaux de E.

Théorème 1.19 *Pour $(E, \langle \cdot \mid \cdot \rangle)$ espace euclidien de dimension $n \geq 1$, $\mathcal{O}(E)$ est un sous-groupe compact de $GL(E)$.*

Démonstration. Soit $u \in \mathcal{O}(E)$. Pour $x \in \ker(u)$, on a $0 = \|u(x)\| = \|x\|$ et $x = 0$. Donc $\ker(u) = \{0\}$ et u est injective, ce qui équivaut à dire que u est un automorphisme de E puisqu'on est en dimension finie.

On a $Id \in \mathcal{O}(E)$ et pour u, v dans $\mathcal{O}(E)$, x dans E, on a :

$$\|u \circ v(x)\| = \|u(v(x))\| = \|v(x)\| = \|x\|$$

$$\left\|u^{-1}(x)\right\| = \left\|u\left(u^{-1}(x)\right)\right\| = \|x\|$$

donc $u \circ v$ et u^{-1} sont dans $\mathcal{O}(E)$. L'ensemble $\mathcal{O}(E)$ est donc bien un sous-groupe de $GL(E)$.

Pour toute isométrie $u \in \mathcal{O}(E)$, on a $\|u(x)\| = \|x\|$ pour tout vecteur x et donc $\|u\| = 1$, c'est-à-dire que $\mathcal{O}(E)$ est contenu dans la sphère unité de $\mathcal{L}(E)$, c'est donc une partie bornée.

Si $(u_p)_{p \in \mathbb{N}}$ est une suite d'éléments de $\mathcal{O}(E)$ qui converge vers $u \in \mathcal{L}(E)$, pour tout $x \in E$, on a alors :

$$\|u(x) - u_p(x)\| = \|(u - u_p)(x)\| \leq \|u - u_p\| \|x\| \underset{p \to +\infty}{\to} 0$$

donc $\lim\limits_{p \to +\infty} u_p(x) = u(x)$ et :

$$\|u(x)\| = \lim_{p \to +\infty} \|u_p(x)\| = \lim_{p \to +\infty} \|x\| = \|x\|$$

et $u \in \mathcal{O}(E)$. L'ensemble $\mathcal{O}(E)$ est donc fermé $\mathcal{L}(E)$.

On peut aussi dire que $\mathcal{O}(E) = \varphi^{-1}\{Id\}$, où φ est l'application continue $\varphi : u \in \mathcal{L}(E) \mapsto {}^t u \circ u \in \mathcal{L}(E)$ (l'expression de cette application dans une base de $\mathcal{L}(E)$ est polynomiale).

En définitive $\mathcal{O}(E)$ est fermé borné dans $\mathcal{L}(E)$, ce qui équivaut à dire qu'il est compact puisque $\mathcal{L}(E)$ est un espace normé de dimension finie. ∎

Réciproquement, on peut vérifier que si G est un sous-groupe compact de $GL(E)$, c'est alors le conjugué d'un sous-groupe de $\mathcal{O}(E)$, c'est-à-dire qu'il existe $u \in GL(E)$ tel que le sous-groupe uGu^{-1} est contenu dans $\mathcal{O}(E)$.

Pour montrer ce résultat, on peut utiliser le théorème de point fixe qui suit.

Théorème 1.20 *Soient $(V, \langle \cdot \mid \cdot \rangle)$ un espace euclidien (de dimension finie), H un sous-groupe compact de $GL(V)$ et K un sous-ensemble non vide de V qui est compact, convexe et stable par tous les éléments de H (i. e. $u(K) \subset K$ pour tout $u \in H$).*
Dans ces conditions, il existe un élément a de K qui est point fixe de tous les éléments de H (i. e. $u(a) = a$ pour tout $u \in H$).

Démonstration. La démonstration se fait en plusieurs étapes.

1. On vérifie que l'application :

$$\begin{array}{rccc} N: & V & \to & \mathbb{R}^+ \\ & x & \mapsto & N(x)=\sup\limits_{u\in H}\|u(x)\| \end{array}$$

est une norme strictement convexe sur V (i. e. une norme telle que l'égalité $N(x+y)=N(x)+N(y)$ est réalisée si, et seulement si, x et y sont positivement liés dans V).
Le fait que l'application N est bien définie est une conséquence de la compacité de H.
En effet, pour x fixé dans V, l'application :

$$\begin{array}{rccc} \varphi_x: & \mathcal{L}(E) & \to & \mathbb{R}^+ \\ & u & \mapsto & \|u(x)\| \end{array}$$

est continue (composée de l'application linéaire, donc continue en dimension finie, $u\mapsto u(x)$ et de la norme $\|\cdot\|$), donc sur le compact H elle est bornée et atteint ses bornes.
Il existe donc, pour tout $x\in H$, un automorphisme $u_x\in H$ tel que $N(x)=\|u_x(x)\|$.
On vérifie facilement que N est une norme.
En effet si $x\in V$ est tel que $N(x)=\|u_x(x)\|=0$, on a alors $x=0$ puisque u_x est un automorphisme de V et il est clair que $N(\lambda x)=|\lambda|N(x)$ et $N(x+y)\leq N(x)+N(y)$ pour tous x,y dans V et λ dans $\mathbb{R}$.
Si x,y dans V sont tels que $N(x+y)=N(x)+N(y)$, on a alors en notant $u=u_{x+y}$:

$$\begin{aligned}\|u(x)\|+\|u(y)\|\leq N(x)+N(x)=N(x+y)&=\|u(x+y)\|\\ &\leq\|u(x)\|+\|u(y)\|\end{aligned}$$

donc $\|u(x+y)\|=\|u(x)\|+\|u(y)\|$ et les vecteurs $u(x)$, $u(y)$ sont positivement liés puisqu'une norme euclidienne est strictement convexe. Il il en résulte alors que x et y sont positivement liés dans V puisque u est un automorphisme de V.

2. On vérifie ensuite qu'il existe un unique vecteur $a\in K$ tel que :

$$N(a)=\inf_{x\in K}N(x)$$

L'existence de a est assurée par la continuité de N (on est en dimension finie) et la compacité de K.
Si b est un autre élément de K tel que $N(b)=\inf\limits_{x\in K}N(x)$, comme K est convexe le milieu $c=\dfrac{1}{2}(a+b)$ du segment $[a,b]$ est aussi dans K et :

$$N(c)=N\left(\frac{1}{2}(a+b)\right)\geq N(a)=\frac{N(a)+N(b)}{2}$$

ce qui équivaut à $N(a+b)=N(a)+N(b)$ puisque N est une norme (on a $N(a+b)\leq N(a)+N(b)\leq N(a+b)$) et revient à dire que a et b sont positivement liés puisque cette norme est strictement convexe. Comme $N(a)=N(b)$, la seule possibilité est $a=b$.

3. Enfin, on vérifie que a est point fixe de tous les éléments de H.
Pour tout $u\in H$, l'application $v\mapsto v\circ u$ réalise une permutation du groupe H, donc :

$$N(u(a))=\sup_{v\in H}\|v\circ u(a)\|=\sup_{w\in H}\|w(a)\|=N(a)$$

avec $u(a)\in K$ puisque K est stable par tous les éléments de H. Par unicité de a dans K, on e déduit que $u(a)=a$.

■

En supposant que $(E, \langle \cdot \mid \cdot \rangle)$ est un espace réel euclidien de dimension $n \geq 1$, nous allons appliquer le théorème précédent à l'espace $V = \mathcal{S}(E)$ des endomorphismes symétriques de E muni du produit scalaire défini par :

$$\forall (u, v) \in \mathcal{S}(E), \ \langle u \mid v \rangle = \mathrm{Tr}(u \circ v)$$

Lemme 1.17 *Si G est un sous-groupe compact de $GL(E)$, son image dans $GL(\mathcal{S}(E))$ par l'application :*

$$\begin{array}{rccc} \varphi : & GL(E) & \to & GL(\mathcal{S}(E)) \\ & u & \mapsto & (v \mapsto u \circ v \circ {}^t u) \end{array}$$

est un sous-groupe compact de $GL(S(E))$.

Démonstration. Pour tout $u \in \mathcal{L}(E)$ et tout $v \in S(E)$, on a ${}^t(u \circ v \circ {}^t u) = u \circ {}^t v \circ {}^t u = u \circ v \circ {}^t u$, donc $u \circ v \circ {}^t u \in \mathcal{S}(E)$ et l'application :

$$\begin{array}{rccc} \varphi : & \mathcal{L}(E) & \to & \mathcal{L}(\mathcal{S}(E)) \\ & u & \mapsto & (v \mapsto u \circ v \circ {}^t u) \end{array}$$

est continue.

En effet, en se donnant une base $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ de E, on lui associe la base $(u_{ij})_{1 \leq i,j \leq n}$ de $\mathcal{L}(E)$ définie par :

$$u_{ij}(e_k) = \delta_{j,k} e_i = \begin{cases} 0 \text{ si } k \neq j \\ e_i \text{ si } k = j \end{cases} \quad (1 \leq i, j, k \leq n)$$

(la matrice E_{ij} dans la base $\mathcal{B}$ de u_{ij} a tous ses termes nuls sauf celui en ligne i et colonne j qui vaut 1, donc $(E_{ij})_{1 \leq i,j \leq n}$ est la base canonique de $\mathcal{M}_n(\mathbb{K})$) et l'expression de φ dans cette base est polynomiale, donc continue.

Pour $u \in GL(E)$, on a $\varphi(u) \in GL(\mathcal{S}(E))$.

L'image $H = \varphi(G)$ du compact G de $GL(E)$ par cette application est donc un compact de $GL(\mathcal{S}(E))$. ■

En utilisant le théorème de Carathéodory qui nous dit que dans un espace euclidien l'enveloppe convexe d'un compact est compacte, on obtient le résultat annoncé.

Théorème 1.21 *Si G est un sous-groupe compact de $GL(E)$, c'est alors le conjugué d'un sous-groupe de $\mathcal{O}(E)$, c'est-à-dire qu'il existe $u \in GL(E)$ tel que le sous-groupe $u^{-1}Gu$ est contenu dans $\mathcal{O}(E)$.*

Démonstration. L'ensemble :

$$C = \left\{ v \circ {}^t v \mid v \in G \right\}$$

est une partie compacte non vide de $\mathcal{S}(E)$ (et même de l'ensemble $\mathcal{S}^{++}(E)$ des automorphismes symétriques définis positifs de E) comme image du compact G par l'application continue $v \in \mathcal{L}(E) \mapsto v \circ {}^t v$ (d'expression polynomiale dans une base).

Cet ensemble est stable par tous les éléments du sous-groupe $H = \varphi(G)$ de $GL(\mathcal{S}(E))$, où φ est définie au lemme précédent.

En effet, pour $u \in G$ et $v \in G$, on a :

$$\varphi(u)\left(v \circ {}^t v\right) = u \circ \left(v \circ {}^t v\right) \circ {}^t u = (u \circ v) \circ {}^t(u \circ v)$$

avec $u\circ v\in G$ (G est un groupe), donc $\varphi(u)(v\circ {}^tv)\in C$.

Comme les applications $\varphi(u)$ sont linéaires, l'enveloppe convexe K de C dans $\mathcal{S}(E)$ est aussi stable par H.

Comme C est contenu dans $\mathcal{S}^{++}(E)$ qui est convexe ($w\in\mathcal{L}(E)$ est symétrique défini positif s'il est symétrique avec $\langle x\mid w(x)\rangle>0$ pour tout $x\in E\setminus\{0\}$), son enveloppe convexe K est aussi dans $\mathcal{S}^{++}(E)$.

On dispose donc de $H=\varphi(G)$ qui est un sous-groupe compact de $GL(\mathcal{S}(E))$, de l'enveloppe convexe K de C qui est un compact de $\mathcal{S}^{++}(E)$ stable par H.

Le théorème précédent nous dit alors qu'il existe w dans $K\subset\mathcal{S}^{++}(E)$ point fixe de tous les éléments de H, soit :

$$\forall v\in G,\ \varphi(v)(w)=v\circ w\circ {}^tv=w$$

En désignant par $u\in\mathcal{S}^{++}(E)\subset GL(E)$ la racine carrée de w, on a $w=u^2=u\circ {}^tu$ et :

$$\forall v\in G,\ v\circ u\circ {}^tu\circ {}^tv=u\circ {}^tu$$

soit :

$$\left(u^{-1}\circ v\circ u\right)\circ {}^t\left(u^{-1}\circ v\circ u\right)=I_d$$

ce qui signifie que $u^{-1}\circ v\circ u\in\mathcal{O}(E)$.

En conséquence $u^{-1}Gu$ est un sous-groupe de $\mathcal{O}(E)$. ■

Exercice 1.21 *Soient n,m deux entiers naturels non nuls. On fait agir le groupe produit $GL_n(\mathbb{K})\times GL_m(\mathbb{K})$ sur l'ensemble $\mathcal{M}_{n,m}(\mathbb{K})$ des matrices à n lignes et m colonnes par :*

$$\forall (P,Q)\in GL_n(\mathbb{K})\times GL_m(\mathbb{K}),\ \forall A\in\mathcal{M}_{n,m}(\mathbb{K}),\ (P,Q)\cdot A=PAQ^{-1}$$

1. *Montrer que les orbites correspondantes sont les ensembles :*

$$\mathcal{O}_r=\{A\in\mathcal{M}_{n,m}(\mathbb{K})\mid \mathrm{rg}(A)=r\}$$

où r est compris entre 0 et $\min(n,m)$.

2. *Pour $\mathbb{K}=\mathbb{C}$, montrer que toutes ces orbites sont connexes par arcs.*

Solution 1.21

1. *Tout est basé sur le fait qu'une matrice $A\in\mathcal{M}_{n,m}(\mathbb{K})$ est de rang r si, et seulement si, elle est équivalente à $A_r=\begin{pmatrix} I_r & 0_{r,m-r}\\ 0_{n-r,r} & 0_{n-r,m-r}\end{pmatrix}$.*

Rappelons une démonstration de ce résultat.

Pour $r=0$, on a $A=0=A_0$.

Pour $r\geq 1$, en désignant par $u\in\mathcal{L}(\mathbb{K}^m,\mathbb{K}^n)$ l'application linéaire de matrice A dans les bases canoniques de $\mathbb{K}^m$ et $\mathbb{K}^n$, H un supplémentaire de $\ker(u)$ dans $\mathbb{K}^m$, $\mathcal{B}_1=(e_i)_{1\leq i\leq r}$ une base de H et $\mathcal{B}_2$ une base de $\ker(u)$, le système $u(\mathcal{B}_1)=(u(e_1))_{1\leq i\leq r}$ qui est libre dans $\mathbb{K}^n$ (si $\sum_{k=1}^{r}\lambda_k u(e_k)=0$, alors $\sum_{k=1}^{r}\lambda_k e_k\in H\cap\ker(u)=\{0\}$ et tous les λ_k sont nuls) se complète en une base $\mathcal{B}=(u(e_1),\cdots,u(e_r),f_{r+1},\cdots,f_n)$ de $\mathbb{K}^n$ et la matrice de u dans les bases $\mathcal{B}_1\cup\mathcal{B}_2$ de $\mathbb{K}^m$ et $\mathcal{B}$ de $\mathbb{K}^n$ a alors la forme indiquée. La réciproque est évidente.

Il en résulte que :

$$\begin{aligned}\mathcal{O}_r&=\{A\in\mathcal{M}_{n,m}(\mathbb{K})\mid \mathrm{rg}(A)=r\}\\&=\left\{A\in\mathcal{M}_{n,m}(\mathbb{K})\mid \exists (P,Q)\in GL_n(\mathbb{K})\times GL_m(\mathbb{K})\mid A=PI_rQ^{-1}\right\}\\&=(GL_n(\mathbb{K})\times GL_m(\mathbb{K}))\cdot I_r\end{aligned}$$

et :

$$\mathcal{M}_{n,m}(\mathbb{K}) = \bigcup_{r=0}^{\min(n,m)} \mathcal{O}_r = \bigcup_{r=0}^{\min(n,m)} (GL_n(\mathbb{K}) \times GL_m(\mathbb{K})) \cdot I_r$$

ce qui nous donne toutes les orbites.

2. *Pour toutes matrices A, B dans $\mathcal{O}_r$ il existe (P, R) dans $GL_n(\mathbb{C}) \times GL_m(\mathbb{C})$ telles que $B = PAR$. Si γ_1 et γ_2 sont deux fonctions continues de $[0,1]$ dans $GL_n(\mathbb{C})$ et $GL_m(\mathbb{C})$ respectivement telles que $\gamma_1(0) = I_n$, $\gamma_2(0) = I_m$, $\gamma_1(1) = P$, $\gamma_2(1) = R$ ($GL_r(\mathbb{C})$ est connexe par arcs) alors $\gamma : t \longmapsto \gamma_1(t) A \gamma_2(t)$ est un chemin continu qui relie A et B dans $\mathcal{O}_r$. Ce qui prouve que $\mathcal{O}_r$ est connexe par arcs.*

1.7 $GL(E)$ pour E de dimension finie ou infinie

1.7.1 Transvections et dilations

Les définitions des transvections et dilatations du paragraphe 1.3 sont valables en dimension finie ou infinie.

E est un $\mathbb{K}$-espace vectoriel normé de dimension finie ou infinie.

Théorème 1.22

1. *Un endomorphisme $u \in \mathcal{L}(E)$ est une transvection si, et seulement si, il existe un hyperplan H de E tel que $u_{|H} = Id_H$ et $\operatorname{Im}(u - Id) \subset H$.*
2. *Une transvection $\tau_{\varphi,a}$ est dans $GL(E)$, son inverse est la transvection $\tau_{\varphi,-a}$, 1 est l'unique valeur propre de $\tau_{\varphi,a}$, l'espace propre associé étant $\ker(\varphi)$ si $u \neq Id$.*
3. *Le conjugué dans $GL(E)$ d'une transvection est une transvection.*
4. *L'ensemble $T(H)$ des transvections d'hyperplan $H = \ker(\varphi)$ est un sous groupe commutatif de $GL(E)$ isomorphe au groupe additif $(H, +)$.*
5. *Une transvection u admet un polynôme minimal qui est $X - 1$ si $u = Id$ ou $(X-1)^2$ si $u \neq Id$.*

Démonstration.

1. Si $u = \tau_{\varphi,a} = Id + \varphi \cdot a$ (avec $\varphi \in E^* \setminus \{0\}$ et $a \in \ker(\varphi)$) est une transvection d'hyperplan $H = \ker(\varphi)$, on a alors :
$$u_{|H} = Id_H + \varphi_{|H} \cdot a = Id_H$$
et pour tout $x \in E$, $(u - Id)(x) = \varphi(x)\, a \in H$, donc $\operatorname{Im}(u - Id) \subset H$.
Réciproquement, supposons qu'il existe un hyperplan $H = \ker(\varphi)$ (avec $\varphi \in E^* \setminus \{0\}$) tel que $u_{|H} = Id_H$ et $\operatorname{Im}(u - Id) \subset H$.
On a $E = H \oplus \mathbb{K}b$, où $b \notin H$.
Comme $\operatorname{Im}(u - Id) \subset H$, on a $a = \dfrac{1}{\varphi(b)}(u(b) - b) \in H$ et :
$$\forall x \in H,\ \tau_{\varphi,a}(x) = x = u(x) \text{ et } \tau_{\varphi,a}(b) = b + \varphi(b)\, a = b + (u(b) - b) = u(b)$$
donc $u = \tau_{\varphi,a}$ est une transvection.

2. Soit $u = \tau_{\varphi,a}$ une transvection d'hyperplan $\ker(\varphi)$.
L'application $v = \tau_{\varphi,-a}$ est une transvection d'hyperplan $\ker(\varphi)$ (on a bien $-a \in \ker(\varphi)$) et pour tout $x \in E$, on a :
$$\begin{aligned} v \circ u(x) &= v(x + \varphi(x)\, a) = v(x) + \varphi(x)\, v(a) \\ &= x - \varphi(x)\, a + \varphi(x)\,(a - \varphi(a)\, a) = x \end{aligned}$$
($\varphi(a) = 0$ puisque $a \in \ker(\varphi)$).
De manière analogue, on vérifie que $u \circ v = Id$.
Donc $\tau_{\varphi,a} \in GL(E)$ et $(\tau_{\varphi,a})^{-1} = \tau_{\varphi,-a}$.
Pour $a = 0$, on a $u = Id$ qui a pour unique valeur propre 1.
Supposons $a \neq 0$. Pour tout scalaire μ, l'équation $u(x) = \mu x$ équivaut à $(1-\mu)\, x + \varphi(x)\, a = 0$.
Pour $\mu = 1$, cela équivaut à $\varphi(x) = 0$, soit à $x \in \ker(\varphi)$., donc 1 est valeur propre de u d'espace propre associé $\ker(\varphi)$.
Pour $\mu \neq 1$, cela équivaut à $x = \dfrac{\varphi(x)}{\mu - 1} a \in \ker(\varphi)$, donc $\varphi(x) = 0$ et $x = 0$. La seule valeur propre de 1 est bien 1.
3. Soient $u = \tau_{\varphi,a}$ une transvection et $v \in GL(E)$. Pour tout $x \in E$, on a :
$$\begin{aligned} v^{-1} \circ \tau_{\varphi,a} \circ v(x) &= v^{-1}(v(x) + (\varphi \circ v)(x)\, a) \\ &= x + (\varphi \circ v)(x)\, v^{-1}(a) = \tau_{\varphi \circ v, v^{-1}(a)}(x) \end{aligned}$$
(on a bien $v^{-1}(a) \in \ker(\varphi \circ v)$ puisque $(\varphi \circ v)(v^{-1}(a)) = \varphi(a) = 0$).
Donc :
$$\forall v \in GL(E),\ v^{-1} \circ \tau_{\varphi,a} \circ v = \tau_{\varphi \circ v, v^{-1}(a)}$$
4. L'identité est la transvection $\tau_{\varphi,0}$, donc $T(H) \neq \emptyset$.
Pour tout $a \in H$, on a vu que l'inverse de la transvection $\tau_{\varphi,a}$ est la transvection $\tau_{\varphi,-a} \in T(H)$.
Pour a, b dans H et $x \in E$, on a :
$$\begin{aligned} \tau_{\varphi,a} \circ \tau_{\varphi,b}(x) &= \tau_{\varphi,a}(x + \varphi(x)\, b) = \tau_{\varphi,a}(x) + \varphi(x)\, \tau_{\varphi,a}(b) \\ &= x + \varphi(x)\, a + \varphi(x)\,(b + \varphi(b)\, a) = x + \varphi(x)\,(a + b) \end{aligned}$$
($\varphi(b) = 0$) donc $\tau_{\varphi,a} \circ \tau_{\varphi,b} = \tau_{\varphi,a+b} = \tau_{\varphi,b+a} \in T(H)$.
L'application $a \in H \mapsto \tau_{\varphi,a} \in T(H)$ réalise un isomorphisme de groupes de $(H, +)$ sur $(T(H), \circ)$ (c'est un morphisme de groupes surjectif et $\tau_{\varphi,a} = Id$ équivaut à $a = 0$).
5. Si $u = Id$, son polynôme minimal est $X - 1$.
Si $u = \tau_{\varphi,a} \neq Id$, on a $u - Id = \varphi \cdot a \neq 0$ et pour tout $x \in E$:
$$(u - Id)^2(x) = (u - Id)(\varphi(x)\, a) = \varphi(x)\,(u - Id)(a)$$
puisque $a \in \ker(\varphi) = \ker(u - Id)$. Donc le polynôme minimal est $(X-1)^2$.

■

Théorème 1.23

1. *Un automorphisme $u \in GL(E)$ est une dilatation si, et seulement si, il existe un hyperplan H de E tel que $u_{|H} = Id_H$ et u est diagonalisable de valeurs propres 1 et $\lambda \in \mathbb{K} \setminus \{0, 1\}$ (c'est-à-dire que $E = \ker(u - Id) \oplus \ker(u - \lambda Id)$).*

2. *Le conjugué dans $GL(E)$ d'une dilatation est une dilatation de même rapport.*
3. *Une dilatation u de rapport λ admet un polynôme minimal qui est $(X-1)(X-\lambda)$.*
4. *L'inverse d'une dilatation de rapport λ est une dilatation de rapport $\dfrac{1}{\lambda}$.*

Démonstration.

1. Soit $u = \delta_{\varphi,a} \in GL(E)$ une dilatation d'hyperplan $H = \ker(\varphi)$ avec $a \notin H$.
On a $\ker(u - Id) = \ker(\varphi \cdot a) = \ker(\varphi)$ puisque $a \in E \setminus H$ est non nul, donc 1 est une valeur propre de u d'espace propre associé $\ker(u - Id) = H$ et $u \neq Id$.
Avec $u(a) = (1 + \varphi(a))\, a$ et $a \neq 0$, on déduit que $\lambda = 1 + \varphi(a) \neq 1$ est valeur propre de u, l'espace propre associé étant $\mathbb{K}a$. ($u(x) = x + \varphi(x)\, a = (1 + \varphi(a))\, x$ équivaut à $x = \dfrac{\varphi(x)}{\varphi(a)} a$) et u est diagonalisable puisque $E = H \oplus \mathbb{K}a$. Comme on a supposé que $u \in GL(E)$, la valeur propre λ est non nulle.
Réciproquement, supposons que $u \in GL(E)$ soit diagonalisable de valeurs propres 1 et $\lambda \in \mathbb{K} \setminus \{0, 1\}$ et qu'il existe un hyperplan $H = \ker(\varphi)$ ($\varphi \in E^* \setminus \{0\}$) tel que $u_{|H} = Id_H$.
Pour $a \in E \setminus \{0\}$ tel que $u(a) = \lambda a$, on a $a \notin H$ (puisque $\lambda \neq 1$ et $u_{|H} = Id_H$), donc $E = H \oplus \mathbb{K}a$. On cherche $b \notin H$ tel que $u = \delta_{\varphi,b}$. Pour tout $x \in H$, on a $\delta_{\varphi,b}(x) = x = u(x)$, quel que soit $b \notin H$. L'égalité $u = \delta_{\varphi,b}$ sera réalisée si, et seulement si, $\delta_{\varphi,b}(a) = u(a)$, ce qui équivaut à $a + \varphi(a)\, b = \lambda a$ et impose $b = \dfrac{\lambda - 1}{\varphi(a)} a$ qui est bien dans $E \setminus H$.
En définitive, $u = \delta_{\varphi,b}$ est une dilatation.
2. Soient $u = \delta_{\varphi,a}$ une dilatation et $v \in GL(E)$. Pour tout $x \in E$, on a :
$$\begin{aligned} v^{-1} \circ \delta_{\varphi,a} \circ v(x) &= v^{-1}(v(x) + (\varphi \circ v)(x)\, a) \\ &= x + (\varphi \circ v)(x)\, v^{-1}(a) = \delta_{\varphi \circ v, v^{-1}(a)} \end{aligned}$$
(on a bien $v^{-1}(a) \notin \ker(\varphi \circ v)$ puisque $(\varphi \circ v)(v^{-1}(a)) = \varphi(a) \neq 0$).
Avec :
$$\varphi \circ v\left(v^{-1}(a)\right) = \varphi(a)$$
on déduit que $v^{-1} \circ \delta_{\varphi,a} \circ v = \delta_{\varphi \circ v, v^{-1}(a)}$ a même rapport que $u = \delta_{\varphi,a}$.
3. Si $u = \delta_{\varphi,a}$, on a alors pour tout $x \in E$:
$$(u - \lambda Id) \circ (u - Id)(x) = (u - \lambda Id)(\varphi(x)\, a) = \varphi(x)(u - \lambda Id)(a) = 0$$
puisque $a \in \ker(u - \lambda Id)$, $u - Id = \varphi \cdot a \neq 0$ et pour tout $h \in H \setminus \{0\}$, $(u - \lambda Id)(h) = (1 - \lambda)\, h \neq 0$ puisque $\lambda \neq 1$, donc $u - \lambda Id \neq 0$ et le polynôme minimal est $(X-1)(X-\lambda)$.
4. Soit $u = \delta_{\varphi,a}$ une dilatation de rapport $\lambda = 1 + \varphi(a)$. En écrivant que $E = H \oplus \mathbb{K}a$ (où $H = \ker(\varphi)$), on a $u(h) = h$ pour tout $h \in H$ et $u(a) = \lambda a$.
L'inverse $v = u^{-1}$ de u est défini par $v(h) = h$ pour tout $h \in H$ et $v(a) = \dfrac{1}{\lambda} a$.
Tout $x \in E$ s'écrit de manière unique $x = h_x + \alpha_x a$ avec $(h_x, \alpha_x) \in H \times \mathbb{K}$ et on a :
$$\begin{aligned} u(x) &= x + \varphi(x)\, a = u(h_x + \alpha_x a) = h_x + \alpha_x \lambda a = h_x + \alpha_x a + (\lambda - 1)\, \alpha_x a \\ &= x + (\lambda - 1)\, \alpha_x a \end{aligned}$$
donc $\varphi(x) = (\lambda - 1)\, \alpha_x$ et :
$$\begin{aligned} v(x) = v(h_x + \alpha_x a) &= x + \left(\frac{1}{\lambda} - 1\right) \alpha_x a \\ &= x + \frac{1 - \lambda}{\lambda} \frac{\varphi(x)}{\lambda - 1} a = x - \frac{\varphi(x)}{\lambda} a = \delta_{-\frac{\varphi}{\lambda}, a}(x) \end{aligned}$$

donc v est une dilatation de rapport $1-\dfrac{\varphi(a)}{\lambda}=1-\dfrac{\lambda-1}{\lambda}=\dfrac{1}{\lambda}$.

On peut aussi utiliser le polynôme minimal $\pi_u(X)=(X-1)(X-\lambda)$ pour calculer u^{-1}. De $u^2-(1+\lambda)u+\lambda Id=0$, on déduit que :

$$\begin{aligned}u^{-1}&=-\frac{1}{\lambda}(u-(1+\lambda)Id)=-\frac{1}{\lambda}(\varphi\cdot a-\lambda Id)\\&=Id-\frac{1}{\lambda}\varphi\cdot a=\delta_{-\frac{\varphi}{\lambda},a}\end{aligned}$$

et v est une dilatation de rapport $1-\dfrac{\varphi(a)}{\lambda}=1-\dfrac{\lambda-1}{\lambda}=\dfrac{1}{\lambda}$.

■

1.7.2 Topologie sur $GL(E)$ ($\mathbb{K}=\mathbb{R}$ ou $\mathbb{K}=\mathbb{C}$)

Pour ce paragraphe, $\mathbb{K}=\mathbb{R}$ ou $\mathbb{K}=\mathbb{C}$ et $(E,\|\cdot\|)$ est un $\mathbb{K}$-espace vectoriel normé de dimension finie ou infinie.

On rappelle que si u un endomorphisme de E, alors les assertions suivantes sont équivalentes :
- u est continue en 0 ;
- u est continue sur E ;
- u est bornée sur la sphère [resp. boule] unité de $(E,\|\cdot\|)$;
- il existe une constante réelle c telle que :

$$\forall x\in E,\ \|u(x)\|\leq c\|x\|$$

- u est uniformément continue sur E.

En notant $\mathcal{L}(E)$ l'espace des applications linéaires continues de E dans E, on peut le munir de la norme définie par :

$$\forall u\in\mathcal{L}(E),\ \|u\|=\sup_{\substack{x\in E\\ \|u\|=1}}\|u(x)\|=\sup_{x\in E\setminus\{0\}}\frac{\|u(x)\|}{\|x\|}$$

On a $\|Id\|=1$ et pour tous u,v dans $\mathcal{L}(E)$, on a $\|u\circ v\|\leq\|u\|\,\|v\|$, ce qui se traduit en disant que $\mathcal{L}(E)$ est une algèbre normée.

$GL(E)$ désigne le groupe des éléments inversibles de $\mathcal{L}(E)$ ($u\in GL(E)$ signifie que u est linéaire, continue, bijective et d'inverse u^{-1} continu).

Dans le cas où l'espace E est de dimension finie, toutes les normes équivalentes et tout endomorphisme est continu.

Pour ce qui suit, on suppose que E est un espace de Banach.

Théorème 1.24 *L'espace $(\mathcal{L}(E),\|\cdot\|)$ des applications linéaires continues de E dans E est une algèbre de Banach.*

Démonstration. On sait déjà que $(\mathcal{L}(E),\|\cdot\|)$ est une algèbre nomée.

Soit $(u_n)_{n\in\mathbb{N}}$ une suite de Cauchy dans $\mathcal{L}(E)$. Avec :

$$\forall x\in E,\ \forall m>n,\ \|u_m(x)-u_n(x)\|\leq\|u_m-u_n\|\,\|x\|$$

on déduit que pour tout x dans E, la suite $(u_n(x))_{n\in\mathbb{N}}$ est de Cauchy dans l'espace de Banach E, elle converge donc vers un élément $u(x)$ de E.

On vérifie facilement que u, qui est limite simple d'applications linéaires, est linéaire.

La suite $(u_n)_{n\in\mathbb{N}}$ qui est de Cauchy dans $\mathcal{L}(E)$ est bornée, ce qui entraîne l'existence d'une constante $M > 0$ telle que tout x dans E, on a :

$$\forall n \in \mathbb{N},\ \forall x \in E,\ \|u_n(x)\| \leq \|u_n\|\,\|x\| \leq M\,\|x\|$$

Avec la continuité de la norme sur E, on en déduit que :

$$\forall x \in E,\ \|u(x)\| = \lim_{n\to+\infty} \|u_n(x)\| \leq M\,\|x\|$$

ce qui signifie que u est continue sur E, donc $u \in \mathcal{L}(E)$.

Il nous reste à vérifier que $u = \lim_{n\to+\infty} u_n$ dans $\mathcal{L}(E)$.

Pour $\varepsilon > 0$ donné, on peut trouver un entier $n_\varepsilon \in \mathbb{N}$ tel que :

$$\forall m > n \geq n_\varepsilon,\ \|u_m - u_n\| < \varepsilon$$

ce qui entraîne :

$$\forall x \in E,\ \forall m > n \geq n_\varepsilon,\ \|u_m(x) - u_n(x)\| \leq \varepsilon\,\|x\|$$

et faisant tendre m vers l'infini dans cette dernière inégalité, on aboutit à :

$$\forall x \in E,\ \forall n \geq n_\varepsilon,\ \|u(x) - u_n(x)\| \leq \varepsilon\,\|x\|$$

et donc :

$$\forall n \geq n_\varepsilon,\ \|u - u_n\| \leq \varepsilon$$

ce qui traduit la convergence de la suite $(u_n)_{n\in\mathbb{N}}$ vers u dans $\mathcal{L}(E)$.

L'espace $\mathcal{L}(E)$ est donc complet. ∎

Lemme 1.18 *Pour tout $u \in \mathcal{L}(E)$ tel que $\|u\| < 1$, l'endomorphisme $Id - u$ est dans $GL(E)$ d'inverse $\sum_{k=0}^{+\infty} u^k$.*

Démonstration. Comme $\|u\| < 1$, la série $\sum \|u\|^k$ est convergente, donc la série $\sum u^k$ est normalement convergente (puisque $\left\|u^k\right\| \leq \|u\|^k$) et convergente dans l'espace de Banach $\mathcal{L}(E)$.

Avec :

$$\left(\sum_{j=0}^{k} u^j\right)(Id - u) = Id - u^{k+1}$$

et $\lim_{k\to+\infty} u^k = 0$ (terme général d'une série convergente), on déduit que :

$$\left(\sum_{k=0}^{+\infty} u^k\right)(Id - u) = Id - \lim_{k\to+\infty} u^{k+1} = Id$$

(continuité du produit comme conséquence de $\|u \circ v\| \leq \|u\|\,\|v\|$), ce qui signifie que $Id - u$ est inversible d'inverse $\sum_{k=0}^{+\infty} u^k$. ∎

Théorème 1.25 *Le groupe $GL(E)$ est ouvert dans $\mathcal{L}(E)$.*

Démonstration. Soient $u \in GL(E)$ et $\delta = \dfrac{1}{\|u^{-1}\|}$.

Pour tout h dans la boule ouverte $B(0,\delta)$, on a :

$$\left\|u^{-1}h\right\| \leq \left\|u^{-1}\right\| \|h\| < 1$$

donc $Id + u^{-1}h \in GL(E)$ et $u + h = u\left(Id + u^{-1}h\right) \in GL(E)$. On a donc $B(u,\delta) \subset GL(E)$ et $GL(E)$ est ouvert dans E. ∎

Exercice 1.22 *Montrer que l'application $u \mapsto u^{-1}$ est continue sur $GL(E)$.*

Solution 1.22 *Soient $u \in GL(E)$ et $\delta = \dfrac{1}{\|u^{-1}\|}$. Pour tout $h \in B(0,\delta)$, on a $u+h \in GL(E)$ et :*

$$\begin{aligned}
\left\|(u+h)^{-1} - u^{-1}\right\| &= \left\|u^{-1}\left(\left(Id + u^{-1}h\right)^{-1} - Id\right)\right\| \\
&= \left\|u^{-1}\left(\sum_{k=1}^{+\infty}(-1)^k\left(u^{-1}h\right)^k\right)\right\| = \left\|u^{-1}\left(u^{-1}h\right)\left(\sum_{k=1}^{+\infty}(-1)^k\left(u^{-1}h\right)^{k-1}\right)\right\| \\
&= \left\|\left(u^{-1}\right)^2 h\left(\sum_{k=0}^{+\infty}(-1)^{k+1}\left(u^{-1}h\right)^k\right)\right\| \\
&\leq \left\|u^{-1}\right\|^2 \|h\| \sum_{k=0}^{+\infty}\left\|u^{-1}h\right\|^k = \frac{\|h\|}{\delta^2}\sum_{k=0}^{+\infty}\left\|u^{-1}h\right\|^k
\end{aligned}$$

Prenant $h \in B\left(0, \dfrac{\delta}{2}\right)$, on a :

$$\left\|u^{-1}h\right\| \leq \left\|u^{-1}\right\| \|h\| < \frac{1}{2}$$

et :

$$\left\|(u+h)^{-1} - u^{-1}\right\| \leq \frac{\|h\|}{\delta^2}\sum_{k=0}^{+\infty}\left(\frac{1}{2}\right)^k = 2\frac{\|h\|}{\delta^2} \underset{h\to 0}{\to} 0$$

ce qui prouve que l'application $u \mapsto u^{-1}$ est continue sur $GL(E)$.

La densité de $GL(E)$ dans $\mathcal{L}(E)$ n'est pas nécessairement acquise en dimension infinie.

Exercice 1.23 *E est l'espace $\mathbb{C}[X]$ normé par :*

$$\forall P = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X],\ \|P\| = \sum_{k=0}^{n}|a_k|$$

1. *Montrer que l'application :*

$$\begin{array}{rccc} u: & \mathbb{C}[X] & \to & \mathbb{C}[X] \\ & P & \mapsto & XP \end{array}$$

   est linéaire et continue.

2. *Montrer que $B(u,1) \cap GL(E) = \emptyset$ et en déduire que $GL(E)$ n'est pas dense dans $\mathcal{L}(E)$.*

Solution 1.23

1. *Il est clair que u est un endomorphisme de E.*
   Pour tout $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$, on a :
   $$\|u(P)\| = \left\| \sum_{k=0}^{n} a_k X^{k+1} \right\| = \sum_{k=0}^{n} |a_k| = \|P\|$$
   donc u est continue et $\|u\| = 1$.
2. *Pour tout $h \in \mathcal{L}(E)$ tel que $\|h\| < 1$, on a $u + h \notin GL(E)$ car le polynôme 1 ne peut avoir d'antécédent par $u + h$.*
   En effet, s'il existe $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$ tel que $1 = (u+h)(P) = XP + h(P)$, on a $P \neq 0$ et :
   $$h(P) = 1 - XP = 1 - \sum_{k=0}^{n} a_k X^{k+1}$$
   donc :
   $$\|h(P)\| = 1 + \sum_{k=0}^{n} |a_k| = 1 + \|P\|$$
   avec :
   $$\|h(P)\| \leq \|h\| \|P\| < \|P\|$$
   puisque $\|h\| < 1$ et $P \neq 0$, ce qui est impossible.
   En conclusion $B(u,1) \cap GL(E) = \emptyset$ et $GL(E)$ n'est pas dense dans $\mathcal{L}(E)$ ($X \subset E$ est dense dans E si, et seulement si, pour tout $a \in E$ et tout $\varepsilon > 0$, $B(a,\varepsilon) \cap X \neq \emptyset$).